Universität Konstanz

Complex theory of modular curves

Some notes for the Master class in Arakelov geometry

Kopenhagen 2023

Anna von Pippich

Version: August 29, 2023

These notes consists in a collection of well-known facts on modular curves and modular forms. For more details, we refer the reader to the vast literature on the topic.
Any mistakes or typos are mine – please let me know if you find any: *anna.pippich@uni-konstanz.de*.

Contents

1. Background material

1.1 The upper half plane and $\mathrm{PSL}_2(\mathbb{R})$

A model of the hyperbolic plane is given by

$$\mathbb{H} = \{z = x + iy \,|\, x, y \in \mathbb{R},\, y > 0\}.$$

The group

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Mat}_2(\mathbb{R}) \,|\, a, b, c, d \in \mathbb{R},\, ad - bc = 1 \right\}$$

acts on $\mathbb{H}$ by fractional linear transformations as follows: for $z \in \mathbb{H}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$, we define

$$\gamma z := \frac{az + b}{cz + d}.$$

We also write $\gamma(z)$ or $\gamma.z$ instead of γz.

The map given by $z \mapsto \gamma z$ ($z \in \mathbb{H}$, $\gamma \in \mathrm{SL}_2(\mathbb{R})$) is also called Moebius transformation. The group of all Moebius transformations $\mathrm{PSL}_2(\mathbb{R})$ satisfies

$$\mathrm{PSL}_2(\mathbb{R}) \simeq \mathrm{SL}_2(\mathbb{R}) / \{\pm\}.$$

To ease notation, elements in $\mathrm{PSL}_2(\mathbb{R})$ will be denoted by matrices in $\mathrm{SL}_2(\mathbb{R})$.

Recall that the modular group is given by

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Mat}_2(\mathbb{Z}) \,|\, a, b, c, d \in \mathbb{Z},\, ad - bc = 1 \right\}.$$

One can consider subgroups $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ of finite index. These are groups such that there is a coset decomposition

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{j=1}^{n} \Gamma g_j$$

for certain $g_1, \ldots, g_n \in \mathrm{SL}_2(\mathbb{Z})$ ($n \in \mathbb{N}$). The subgroups of finite index play a fundamental role in the theory of modular forms.

Lemma 1.1. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ and $z \in \mathbb{H}$, we define $\gamma z := \frac{az+b}{cz+d}$. Then, for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ and $z \in \mathbb{H}$, we have

(i)
$$\mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \frac{\mathrm{Im}(z)\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}{|cz+d|^2}.$$
Hence, if $\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = ad - bc > 0$, then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z \in \mathbb{H}$.

(ii) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} z = z.$

(iii) $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) z\right) = \left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)\right) z.$

In particular, the modular group $\mathrm{SL}_2(\mathbb{Z})$ and the subgroup $\mathrm{GL}_2^+(\mathbb{R})$ of $\mathrm{GL}_2(\mathbb{R})$ of matrices with positive determinant both act on $\mathbb{H}$.

Proof. Exercise. ■

The group $\mathrm{SL}_2(\mathbb{R})$ acts transitively on $\mathbb{H}$, since if $z = x + iy \in \mathbb{H}$ we have $\gamma i = z$ for

$$\gamma = \begin{pmatrix} \sqrt{y} & \frac{x}{\sqrt{y}} \\ 0 & \sqrt{y} \end{pmatrix}.$$

The stabilizer group

$$K := \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{R})}(i) = \{\gamma \in \mathrm{SL}_2(\mathbb{R}) \mid \gamma.i = i\}$$

is given by the special orthogonal group

$$K = \left\{k(2\theta) := \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \mid 0 \leq \theta < 2\pi\right\}$$

The element $k(2\theta)$ acts on $\mathbb{H}$ by a hyperbolic rotation at i of angle 2θ. One gets

$$\mathbb{H} \simeq \mathrm{SL}_2(\mathbb{R})/K,$$

where $z = x + iy$ corresponds to the right coset

$$\begin{pmatrix} \sqrt{y} & \frac{x}{\sqrt{y}} \\ 0 & \sqrt{y} \end{pmatrix} K \in \mathrm{SL}_2(\mathbb{R})/K.$$

We want to extend the action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$ to the extended upper half plane

$$\mathbb{H}^* := \mathbb{H} \cup \mathbb{R} \cup \{\infty\} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{R}).$$

We write an element of $\mathbb{P}^1(\mathbb{R})$ as $[r : s]$ with $r, s \in \mathbb{R}$, not both equal to 0. We define

$$\gamma[r : s] := [ar + bs : cr + ds]$$

for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$. We also write $\gamma([r : s])$ or $\gamma.[r : s]$ instead of $\gamma[r : s]$.

Let $[0 : 1] =: 0$ and $[1 : 0] =: \infty$. The group $\mathrm{SL}_2(\mathbb{R})$ acts doubly transitively on $\mathbb{P}^1(\mathbb{R})$, i.e. for $[r_1 : s_1], [r_2 : s_2] \in \mathbb{P}^1(\mathbb{R})$ there exists $\sigma \in \mathrm{SL}_2(\mathbb{R})$ such that

$$\sigma.0 = [r_1 : s_1] \text{ and } \sigma.\infty = [r_2 : s_2].$$

The hyperbolic line element ds^2_{hyp} is given by

$$ds^2_{\mathrm{hyp}} = \frac{dx^2 + dy^2}{y^2}.$$

It is invariant under the action of $\mathrm{SL}_2(\mathbb{R})$.

Moreover, for $z_1, z_2 \in \mathbb{H}$, we have

$$d_{\mathrm{hyp}}(\gamma z_1, \gamma z_2) = d_{\mathrm{hyp}}(z_1, z_2)$$

for any $\gamma \in \mathrm{SL}_2(\mathbb{R})$, i.e. the elements of $\mathrm{SL}_2(\mathbb{R})$ act as isometries on $\mathbb{H}$ (with respect to the hyperbolic metric). Here, the hyperbolic distance $d_{\mathrm{hyp}}(z_1, z_2)$ $(z_1, z_2 \in \mathbb{H})$ is given by

$$d_{\mathrm{hyp}}(z_1, z_2) = \inf_{\gamma} \left(\int_{\gamma} ds^2_{\mathrm{hyp}} \right)^{\frac{1}{2}},$$

where γ runs over all continuous paths $\gamma : [0,1] \longrightarrow \mathbb{H}$ with $\gamma(0) = z_1$, $\gamma(1) = z_2$.
We have (see Beardon : "Geometry of discrete groups, p. 131) for $z_1, z_2 \in \mathbb{H}$

$$d_{\mathrm{hyp}}(z_1, z_2) = \log \left(\frac{|z_1 - \bar{z_2}| + |z_1 - z_2|}{|z_1 - \bar{z_2}| - |z_1 - z_2|} \right)$$

and the useful identity

$$\cosh(d_{\mathrm{hyp}}(z_1, z_2)) = 1 + 2u(z_1, z_2),$$

with

$$u(z_1, z_2) := \frac{|z_1 - z_2|^2}{4\mathrm{Im}(z_1)\mathrm{Im}(z_2)}$$

and $\cosh(x) := \frac{e^x + e^{-x}}{2}$.
The hyperbolic Laplacian on $\mathbb{H}$ is defined by

$$\Delta_{\mathrm{hyp}} := -y^2 \left(\frac{\partial}{\partial x^2} + \frac{\partial}{\partial y^2} \right).$$

It is $\mathrm{SL}_2(\mathbb{R})$ invariant. Finally, the hyperbolic volume element on $\mathbb{H}$ is given by

$$\mu_{\mathrm{hyp}}(z) = \frac{dx \wedge dy}{y^2},$$

which is also $\mathrm{SL}_2(\mathbb{R})$ invariant.

The Iwasawa decomposition refines the identification $\mathbb{H} \cong \mathrm{SL}_2(\mathbb{R})/K$ as follows: We define the subgroups

$$N := \left\{ n(\zeta) := \begin{pmatrix} 1 & \zeta \\ 0 & 1 \end{pmatrix} \mid \zeta \in \mathbb{R} \right\}$$
$$A := \left\{ a(\mu) := \begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix} \mid \mu \in \mathbb{R},\, \mu > 0 \right\}.$$

The subgroup A acts on $\mathbb{H}$ by dilations, N by translations. The Iwasawa decomposition states that every $\gamma \in \mathrm{SL}_2(\mathbb{R})$ can be uniquely written as

$$\gamma = nak \text{ with } n \in N,\, a \in K,\, k \in K.$$

That is $\mathrm{SL}_2(\mathbb{R}) = NAK$. In particular the right coset $\gamma K \in \mathrm{SL}_2(\mathbb{R})/K$ which corresponds to $z = x + iy \in \mathbb{H}$ can be written as

$$\gamma K = n(x)a(\sqrt{y})K.$$

1.2 Classification of isometries

By
$$[\gamma] := \{\sigma\gamma\sigma^{-1} | \sigma \in \mathrm{PSL}_2(\mathbb{R})\}$$
we denote the conjugacy class of γ in $\mathrm{PSL}_2(\mathbb{R})$. If $z \in \mathbb{H}^*$ is a fixed point of $\gamma \in \mathrm{PSL}_2(\mathbb{R})$ (i.e. $\gamma z = z$), then σz is a fixed point of $\sigma\gamma\sigma^{-1}$. Therefore the number of fixed points for $\gamma \in \mathrm{PSL}_2(\mathbb{R})$ is invariant under conjugation of γ by elements of $\mathrm{PSL}_2(\mathbb{R})$. If $\gamma = \mathrm{id}$, every $z \in \mathbb{H}^*$ is a fixed point of γ.
If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{R})$, $\gamma \neq \mathrm{id}$, the fixed point equation

$$z = \gamma z \iff cz^2 + (d-a)z - b = 0$$

is quadratic and we obtain the following cases :

(a)

$$\begin{aligned} \gamma \text{ is elliptic} &\iff |tr(\gamma)| < 2 \\ &\iff \gamma \text{ has exactly one fixed point in } \mathbb{H} \text{ (and one in } -\mathbb{H}) \\ &\iff [\gamma] = [k(2\theta)] \text{ for some } \theta \in [0, \pi] \end{aligned}$$

An elliptic element acts as a hyperbolic rotation centered at the (unique) fixed point of γ in $\mathbb{H}$.

(b)

$$\begin{aligned} \gamma \text{ is parabolic} &\iff |tr(\gamma)| = 2 \\ &\iff \gamma \text{ has exactly one fixed point in } \mathbb{P}^1(\mathbb{R}) \\ &\iff [\gamma] = [n(1)] \end{aligned}$$

A parabolic element moves points along horocycles i.e. circles in $\mathbb{H}$ tangent to $\mathbb{P}^1(\mathbb{R})$.

(c)

$$\begin{aligned} \gamma \text{ is hyperbolic} &\iff |tr(\gamma)| > 2 \\ &\iff \gamma \text{ has exactly two fixed points in } \mathbb{P}^1(\mathbb{R}) \\ &\iff [\gamma] = [a(\mu)] \text{ for some } \mu \in \mathbb{R}_{>0} \end{aligned}$$

A hyperbolic element acts as a dilatation, one fixed point is repelling, one is attracting.
This classification is invariant under conjugation.

A fixed point $z \in \mathbb{H}^*$ of a parabolic, hyperbolic or elliptic $\gamma \in \mathrm{PSL}_2(\mathbb{R})$ is called parabolic, hyperbolic or elliptic fixed point.

1.3 Fuchsian groups of the first kind

The group $\mathrm{SL}_2(\mathbb{R})$ can be identified as a topological space with the subset $\{(a,b,c,d) \in \mathbb{R}^4 | \, ad - bc = 1\}$ of $\mathbb{R}^4$. It is a (locally compact) topological group (hausdorff, matrix multiplication and inversion are continuous) with respect to the metric induced by the norm
$$||\gamma|| := (a^2 + b^2 + c^2 + d^2)^{\frac{1}{2}}.$$
This is also true for $\mathrm{PSL}_2(\mathbb{R})$.

Definition 1.2. A Fuchsian subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$, that means that $\{\gamma \in \Gamma \mid ||\gamma|| < k\}$ is finite for every $k > 0$. Every Fuchsian subgroup of $\mathrm{PSL}_2(\mathbb{R})$ is therefore countable.

Fact. $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ is a Fuchsian subgroup if and only if Γ acts properly disontinuously on $\mathbb{H}$, i.e. for any $z_1, z_2 \in \mathbb{H}$ there exist neighbourhoods $U \ni z_1$, $V \ni z_2$ s.t.

$$\#\{\gamma \in \Gamma \mid \gamma U \cap v \neq \varnothing\} < \infty.$$

This implies that the orbit Γz of $z \in \mathbb{H}$ under a Fuchsian subgroup Γ is a discrete set in $\mathbb{H}$. A possible limit point of an orbit Γz for $z \in \mathbb{H}$ can therefore only lie in $\mathbb{P}^1(\mathbb{R})$.
A Fuchsian subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ is called of the first kind if every point in $\mathbb{P}^1(\mathbb{R})$ is a limit point of an orbit Γz for some $z \in \mathbb{H}$.

A Fuchsian subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ can be visualized by a "fundamental domain".

Definition 1.3. Let $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ be a Fuchsian subgroup. A subset $\mathcal{F}_\Gamma \subseteq \mathbb{H}$ is called fundamental domain for Γ if
(a) $\mathcal{F}_\Gamma \subseteq \mathbb{H}$ is a domain (non-empty and open)
(b) Distinct points $z_1 \neq z_2$ of $\mathcal{F}_\Gamma$ are not equivalent with respect to Γ, i.e. $\nexists \gamma \in \Gamma : \gamma z_1 = z_2$
(c) Every orbit Γz, $z \in \mathbb{H}$, contains a point in the closure $\overline{\mathcal{F}_\Gamma}$.

Every Fuchsian subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbb{Z})$ admits a fundamental domain $\mathcal{F}_\Gamma$. A fundamental domain is not unique but all fundamental domains for a fixed Fuchsian subgroup Γ have the same hyperbolic volume

$$\mathrm{vol}_{\mathrm{hyp}}(\mathcal{F}_\Gamma) = \int_{\mathcal{F}_\Gamma} \frac{dxdy}{y^2}.$$

which can be infinite. However:
Fact. $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ is a Fuchsian subgroup of the first kind if and only if the hyberbolic volume $\mathrm{vol}_{\mathrm{hyp}}(\mathcal{F}_\Gamma) < \infty$.

■ **Example 1.4.** (a) The group

$$\Gamma := < \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} >$$

is a Fuchsian subgroup (which is not of the first kind). A fundamental domain is given by

$$\mathcal{F}_\Gamma = \{z \in \mathbb{H} \mid |Re(z)| < \frac{1}{2}\}.$$

We calculate $\mathrm{vol}_{\mathrm{hyp}}(\mathcal{F}_\Gamma) = \int_{\mathcal{F}_\Gamma} \frac{dxdy}{y^2} = \infty$.
(b) The group

$$\Gamma = \mathrm{PSL}_2(\mathbb{Z}) = < \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} >$$

is a Fuchsian group of the first kind. A fundamental domain is given by

$$\mathcal{F}_\Gamma = \{z \in \mathbb{H} \mid |\mathrm{Re}(z)| < \frac{1}{2}, |z| > 1\}.$$

One can calculate that $\mathrm{vol}_{\mathrm{hyp}}(\mathcal{F}_\Gamma) = \frac{\pi}{3}$.

■

Definition 1.5. When $z \in \mathbb{H} \cup \mathbb{P}^1(\mathbb{R})$ is a fixed point of an elliptic, parabolic or hyperbolic element of Γ, we say that z is an elliptic, parabolic or hyperbolic fixed point. A parabolic fixed point of Γ is also called cusp of Γ.

Definition 1.6. The Γ-orbit of an elliptic, parabolic or hyperbolic fixed point of Γ is called elliptic, parabolic or hyperbolic fixed point of $\Gamma \setminus \mathbb{H}$. Parabolic points of $\Gamma \setminus \mathbb{H}$ are called cusps of $\Gamma \setminus \mathbb{H}$.

Remark. The number of cusps and elliptic points of $\Gamma \setminus \mathbb{H}$ is finite.

Lemma 1.7. The set of cusps of $\mathrm{PSL}_2(\mathbb{Z})$ is $\mathbb{Q} \cup \{\infty\} \cong \mathbb{P}^1(\mathbb{Q})$ and all cusps of $\mathrm{PSL}_2(\mathbb{Z})$ are $\mathrm{PSL}_2(\mathbb{Z})$-equivalent, i.e. the number of cusps of $\mathrm{PSL}_2(\mathbb{Z}) \setminus \mathbb{H}$ equals one.

Proof. By the classification of isometries, we know that every cusp is an element of $\mathbb{P}^1(\mathbb{R})$, since a parabolic element has exactly one fixed point and it lies in $\mathbb{P}^1(\mathbb{R})$. Clearly, we have that $\infty = [1:0]$ is a cusp of $\mathrm{PSL}_2(\mathbb{Z})$, since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.[1:0] = [1:0].$$

Let $[r:s] \in \mathbb{P}^1(\mathbb{R})$ with $s \neq 0$, be a cusp of $\mathrm{PSL}_2(\mathbb{Z})$. Then $[r:s] = [\frac{r}{s}:1]$. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{Z})$ be parabolic with

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).[\frac{r}{s}:1] = [\frac{r}{s}:1].$$

This is equivalent to $[a\left(\frac{r}{s}\right)+b : c\left(\frac{r}{s}\right)+d] = [\frac{r}{s}:1]$, which is again equivalent to

$$\frac{a\left(\frac{r}{s}\right)+b}{c\left(\frac{r}{s}\right)+d} = \frac{r}{s},$$

i.e. $\frac{r}{s}$ is a solution of a quadratic equation with rational coefficients, therefore $\frac{r}{s} \in \mathbb{Q}$. On the other hand every element $[q:1] \in \mathbb{P}^1(\mathbb{Q})$ with $q \in \mathbb{Q}$ is a cusp since it is $\mathrm{PSL}_2(\mathbb{Z})$-equivalent to $[1:0]$. To see this let $[a:c] \in \mathbb{P}^1(\mathbb{Q})$ with $c \neq 0$. We can assume that gcd(a,c) = 1. The euclidean algorithm gives us integers $b, d \in \mathbb{Z}$ such that $ad - bc = 1$. But then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.[1:0] = [a:c]$$

and therefore

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}.[a:c] = [a:c].$$

Hence $[a:c]$ is a cusp. This completes the proof is finished. ■

2. Modular curves

2.1 The Riemann surface $\Gamma \backslash \mathbb{H}^*$

From now on let $\Gamma \subset \mathrm{PSL}_2(\mathbb{Z})$ be a subgroup of finite index (for example $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ or $\Gamma = \Gamma_0(N)$, $N \in \mathbb{N}$).

Remark. Since Γ is a subset of $\mathrm{PSL}_2(\mathbb{Z})$ it is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$ and acts therefore properly discontinuously on $\mathbb{H}$, i.e. for any two compact sets K_1, K_2 in $\mathbb{H}$ we have that $\#\{\gamma \in \Gamma \mid \gamma K_1 \cap K_2\} < \infty$.

Definition 2.1. We set

$$\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\} \cong \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

Elements of $\mathbb{H}$ are called *interior points*, elements of $\mathbb{P}^1(\mathbb{Q})$ are called *cusps*.

Remark. $\mathbb{H}^*$ is a topological Hausdorff space, if one installs the following topology :
For an interior point $z \in \mathbb{H}$, a fundamental system of neighbourhoods is defined in the same way as in $\mathbb{H}$.
For $[1 : 0] = \infty$ we can take the sets

$$\{z \in \mathbb{H} \mid \mathrm{Im}(z) > c\},\ c > 0$$

as a fundamental system of neighbourhoods.
For $[r : s] \in \mathbb{P}^1(\mathbb{Q})$, $s \neq 0$, we can take sets

$$\{\text{interior of circles in } \mathbb{H} \text{ tangent to } [r : s]\} \cup \{\infty\}.$$

By construction the topology on $\mathbb{H}^*$ generated by these open sets is Hausdorff.

Definition 2.2. The *stabilizer subgroup* of $z \in \mathbb{H}^*$ in Γ is defined as

$$\Gamma_z := \mathrm{Stab}_\Gamma(z) = \{\gamma \in \Gamma \mid \gamma z = z\}.$$

■ **Example 2.3.** (i) $\mathrm{PSL}_2(\mathbb{Z})_\infty \cong < \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} >$

(ii) If $\Gamma \subset \mathrm{PSL}_2(\mathbb{Z})$ is of finite index, then $\Gamma_\infty \cong < \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} >$ for some $h \in \mathbb{N}$. Then number h is called width of ∞.

■

Remark. Consider the orbit space

$$\Gamma \backslash \mathbb{H}^* = \{\Gamma z \mid z \in \mathbb{H}^*\}.$$

It is a topological space in the following way : if

$$\pi : \mathbb{H}^* \longrightarrow \Gamma \backslash \mathbb{H}^*$$

denotes the canonical projection, then the quotient topology on $\Gamma \backslash \mathbb{H}^*$ is defined by calling a subset $U \subseteq \Gamma \backslash \mathbb{H}^*$ open if and only if $\pi^{-1}(U) \subseteq \mathbb{H}^*$ is open.

In this chapter we want to prove that the topological space $\Gamma \backslash \mathbb{H}^*$ has the structure of a Riemann surface. To do this, we first prove that $\Gamma \backslash \mathbb{H}^*$ is a Hausdorff space. This is clearly true for $\Gamma \backslash \mathbb{H} \subseteq \Gamma \backslash \mathbb{H}^*$, since Γ acts properly discontinuously on $\mathbb{H}$ (because it is discrete). It remains to show that you can seperate:

(a) points in $\Gamma \backslash \mathbb{H}$ and orbits of cusps
(b) different orbits of cusps.

Proposition 2.4. For any cusp $[r : s] \in \mathbb{P}^1(\mathbb{Q})$ and every compact set $K \subseteq \mathbb{H}$ there exists a neighbourhood $\mathbb{H}^* \supset U \ni [r : s]$ such that $U \cap \gamma K = \varnothing$ for all $\gamma \in \Gamma$.

Proof. Without loss of generality we can assume that $[r : s] = [1 : 0] = \infty$. We are going to prove the claim in 4 four steps :

Claim 1: Let $M > 0$. Then there exist only finitely many double cosets $\Gamma_\infty \gamma \Gamma_\infty$ $(\gamma \in \Gamma)$, such that $|c_\gamma| \leq M$, where

$$\gamma = \begin{pmatrix} \star & \star \\ c_\gamma & \star \end{pmatrix}.$$

Proof of Claim 1: Left as an exercise.

Claim 2: For any $\gamma \in \Gamma \setminus \Gamma_\infty$ we have that

$$|c_\gamma| > r$$

for a fixed $r = r(\Gamma) > 0$, which only depends on the group Γ. Additionaly we have

$$\mathrm{Im}(z)\mathrm{Im}(\gamma z) \leq \frac{1}{r^2}.$$

for any $z \in \mathbb{H}$.

Proof of Claim 2: Let $M > 0$ be fixed. Consider the finitely many double cosets

$$\Gamma_\infty \gamma_1 \Gamma_\infty, \ldots, \Gamma_\infty \gamma_n \Gamma_\infty.$$

from claim 1. Then for $\gamma \in \left(\bigcup_{j=1}^{n} \Gamma_\infty \gamma_j \Gamma_\infty\right) \setminus \Gamma_\infty$ we have $|c_\gamma| < M$. Since $c_\gamma \in \{c_{\gamma_1}, \dots, c_{\gamma_n}\}$ we define

$$r := \frac{1}{2} \min\{|c_{\gamma_i}| \mid i = 1, \dots, n\}.$$

We have $r > 0$, since otherwise $\gamma \in \Gamma_\infty$, which contradicts our assumption. Obviously $|c_\gamma| > r$.

Now let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \setminus \Gamma_\infty$. Then $c \neq 0$ and for any $z \in \mathbb{H}$ it holds that

$$\operatorname{Im}(\gamma z) = \frac{\operatorname{Im}(z)}{|cz+d|^2} \overset{c\neq 0}{\leq} \frac{\operatorname{Im}(z)}{c^2 \operatorname{Im}(z)^2} \leq \frac{1}{r^2 \operatorname{Im}(z)},$$

which proves the second claim.

Claim 3: There exists a neighbourhood $\mathbb{H}^* \subset U \ni [1:0] = \infty$ with

$$\Gamma_\infty = \{\gamma \in \Gamma \mid \gamma U \cap U \neq \varnothing\}.$$

Proof of Claim 3: Let

$$U := \left\{ z \in \mathbb{H}^* \mid \operatorname{Im}(z) > \frac{1}{r} \right\}$$

with $r > 0$ from claim 2. Then

$$\Gamma_\infty \subseteq \{\gamma \in \Gamma \mid \gamma U \cap U \neq \varnothing\}.$$

Moreover for any $\gamma \in \Gamma \setminus \Gamma_\infty$, $z \in U$, we have the estimate

$$\operatorname{Im}(\gamma z) \leq \frac{1}{r^2 \operatorname{Im}(z)^2} \underset{z \in U}{\leq} \frac{1}{r^2},$$

i.e. $\gamma z \in U$, hence $\gamma U \cap U \neq \varnothing$. This proves claim 3.

Claim 4: Let $z \in \mathbb{H}$. The orbits $\pi(z) = \Gamma z$ and $\pi(\infty) = \Gamma\infty$ have disjoint neighbourhoods.

Proof: Let $K \subseteq \mathbb{H}$ be compact. We choose $A, B > 0$, such that

$$A < \operatorname{Im}(z) < B$$

for all $z \in K$. Furthermore we define

$$U := \left\{ z \in \mathbb{H}^* \mid \operatorname{Im}(z) > \max\left\{ B, \frac{1}{Ar^2} \right\} \right\},$$

where $r > 0$ comes from claim 2. Therefore for any $\gamma \in \Gamma \setminus \Gamma_\infty$ and any $z \in K$ we get

$$\operatorname{Im}(\gamma z) < \frac{1}{Ar^2}.$$

On the other hand

$$\operatorname{Im}(\gamma z) = \operatorname{Im}(z) < B$$

for any $\gamma \in \Gamma_\infty$ and any $z \in K$. Overall we proved that

$$U \cap \gamma K = \varnothing$$

for all $\gamma \in \Gamma$. This proves claim 4.

This finishes the proof of Proposition 2.4. ∎

Proposition 2.5. The Hausdorff space $\Gamma\backslash\mathbb{H}^*$ is compact.

Proof. Let $(U_j)_{j\in J}$ be an open covering of $\Gamma\backslash\mathbb{H}^*$. Then

$$(\pi^{-1}(U_j)_{j\in J})$$

is an open covering of $\mathbb{H}^*$. Therefore there exists $j_1 \in J$ with $\infty \in \pi^{-1}(U_{j_1})$. Therefore there exists $C > 0$ such that

$$\pi^{-1}(U_{j_1}) \supseteq \{z \in \mathbb{H} \,|\, \mathrm{Im}(z) > C\} \cup \{\infty\},$$

since the sets $\{z \in \mathbb{H} \,|\, \mathrm{Im}(z) > M\} \cup \{\infty\}$, $M > 0$, form a neighbourhood base of ∞ in $\mathbb{H}^*$. Hence $\overline{\mathcal{F}_\Gamma} \setminus \pi^{-1}(U_{j_1})$ is compact (closed and bounded). Therefore there exist $j_2, \ldots, j_n$ in J such that

$$\overline{\mathcal{F}_\Gamma} \setminus \pi^{-1}(U_{j_1}) \subseteq \pi^{-1}(U_{j_2}) \cup \ldots \cup \pi^{-1}(U_{j_n})$$

Since $\pi(\overline{\mathcal{F}_\Gamma}) = \Gamma\backslash\mathbb{H}^*$, we have that

$$\Gamma\backslash\mathbb{H}^* = U_{j_1} \cup \ldots \cup U_{j_n},$$

which proves that $\Gamma\backslash\mathbb{H}^*$ is compact. ■

Recall. A Riemann surface is a connected, topological Hausdorff space X, endowed with a complex structure $\mathcal{S}$ (also called "atlas") given by

$$\mathcal{S} = (U_\alpha, \varphi_\alpha)_{\alpha\in I},$$

where I is an index set, $(U_\alpha)_{\alpha\in I}$ is an open covering of X and

$$\varphi_\alpha : U_\alpha \longrightarrow \varphi_\alpha(U_\alpha) \subset \mathbb{C}$$

is a homeomorphism for every $\alpha \in I$. Furthermore if $\alpha, \beta \in I$ with $U_\alpha \cap U_\beta \neq \varnothing$ the map

$$\varphi_\beta \circ \varphi_\alpha^{-1} : \varphi_\alpha(U_\alpha \cap U_\beta) \longrightarrow \varphi_\beta(U_\alpha \cap U_\beta)$$

is required to be biholomorphic. Finally, $\mathcal{S}$ has to be maximal with these properties.

Proposition 2.6. $\Gamma\backslash\mathbb{H}^*$ is a Riemann surface.

Proof. We have to construct an atlas.

1. case: $\pi(z) \in \Gamma\backslash\mathbb{H}^*$ with $\Gamma_z = \{\mathrm{id}\}$, so especially $z \in \mathbb{H}$. We choose a neighbourhood $U_z \subset \mathbb{H}$ of z such that

$$\Gamma_z = \{\gamma \in \Gamma \,|\, \gamma U_z \cap U_z \neq \varnothing\}.$$

The existence of such a neighbourhood can be seen by a similar argument as in the proof of claim 3 in Proposition 2.4. Then we have

$$\Gamma\backslash\mathbb{H}^* \supseteq \Gamma_z \setminus U_z \xleftarrow[\cong]{\pi} U_z \subset \mathbb{H} \subset \mathbb{C}.$$

Therefore we choose

$$(\Gamma_z \setminus U_z, \pi^{-1})$$

as a chart for $\pi(z)$.

2. *case:* $\pi(z) \in \Gamma\backslash\mathbb{H}^*$ with $\Gamma_z \cong \mathbb{Z}/d\mathbb{Z}$ $(d \in \mathbb{N},\, d > 1)$, so especially $z \in \mathbb{H}$. Let U_z be defined as in the first case. Now consider the biholomorphic mapping

$$\begin{aligned} \lambda : \mathbb{H} &\longrightarrow \mathbb{D} = \{\omega \in C \,|\, |\omega| < 1\} \\ z' &\longmapsto \frac{z' - z}{z' - \overline{z}}. \end{aligned}$$

Obviously we have $\lambda(z) = 0$. Therefore

$$\lambda \circ \Gamma_z \circ \lambda^{-1} = \{[\mathbb{D} \ni \omega \mapsto e^{\frac{2\pi i j \omega}{d}}] \,|\, j = 1, \ldots d-1\}$$

and we obtain a homeomorphism

$$\begin{aligned} \varphi_z : \Gamma\backslash\mathbb{H}^* \supseteq \Gamma_z \setminus U_z &\longrightarrow \mathbb{C} \\ \pi(z') &\longmapsto \lambda(z')^d \end{aligned}$$

Thus we choose the chart $(\Gamma_z \setminus U_z, \varphi_z)$ for $\pi(z)$.

3. *case:* $\pi(z) \in \Gamma\backslash\mathbb{H}^*$ is a cusp, i.e. in particular $z \in \mathbb{P}^1(\mathbb{Q})$. Without loss of generality we can assume $z = \infty = [1:0]$. Then

$$< \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} > \cong \Gamma_\infty$$

for some $h \in \mathbb{N}$.
We choose $U_\infty = \{z \in \mathbb{H} \,|\, \mathrm{Im}(z) > \frac{1}{r}\} \cup \{\infty\}$ with $r > 0$ as in Proposition 2.4, claim 2. Then

$$\Gamma\backslash\mathbb{H}^* \supseteq \Gamma_\infty \setminus U_\infty \cong \left\{ z \in \mathbb{H} \,|\, -\frac{h}{2} \leq Re(z) < \frac{h}{2}, \mathrm{Im}(z) > \frac{1}{r} \right\} \cup \{\infty\}.$$

With the holomorphic map

$$\begin{aligned} \varphi_\infty : \mathbb{H}^* &\longrightarrow \mathbb{C} \\ z &\longmapsto e^{\frac{2\pi i z}{h}} \end{aligned}$$

we find the chart $(\Gamma_\infty \setminus U_\infty, \varphi_\infty)$ for ∞. The proof that this atlas satisfies the compability requirements is left as an exercise. ∎

Remark. A fundamental domain is a connected subset $\mathcal{F}_\Gamma \subset \mathbb{H}^*$ such that there is a bijection $\mathcal{F}_\Gamma \cong \Gamma\backslash\mathbb{H}^*$. From now on we are going to use this new definition (it turns out that this definition is easier to work with in technical proofs).

Remark. **(a)** Let $\Gamma, \Gamma' \subseteq \mathrm{PSL}_2(\mathbb{Z})$ be subgroups of finite index and let $\Gamma' \subseteq \Gamma$. Then there is a natural projection

$$\pi_{\Gamma',\Gamma} : \Gamma' \setminus \mathbb{H}^* \longrightarrow \Gamma\backslash\mathbb{H}^*$$

and we have the following commutative diagramm :

$$\begin{tikzcd} \mathbb{H}^* \arrow[r, "id"] \arrow[d, "\pi_{\Gamma'}"] & \mathbb{H}^* \arrow[d, "\pi_\Gamma"] \\ \Gamma' \setminus \mathbb{H}^* \arrow[r, "\pi_{\Gamma',\Gamma}"] & \Gamma\backslash\mathbb{H}^* \end{tikzcd}$$

(b) The number of cusps of $\Gamma\backslash\mathbb{H}^*$ is finite.

Lemma 2.7. Let $\Gamma, \Gamma' \subseteq \mathrm{PSL}_2(\mathbb{Z})$ be subgroups of finite index and let $\Gamma' \subseteq \Gamma$. Then the Riemann surface $\Gamma' \setminus \mathbb{H}^*$ is a (branched) covering space of the Riemann surface $\Gamma \backslash \mathbb{H}^*$ of degree $N := [\Gamma : \Gamma']$.

Proof. The natural projection $\pi_{\Gamma',\Gamma}$ from the last remark is surjective and holomorphic. It is a local isomorphism and has degree $[\Gamma : \Gamma']$. ∎

Now we want to study the covering $\Gamma \backslash \mathbb{H}^* \longrightarrow \mathrm{PSL}_2(\mathbb{Z}) \setminus \mathbb{H}^*$ for arbitrary $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ of finite index.

Proposition 2.8. The fixed points of $\Gamma := \mathrm{PSL}_2(\mathbb{Z})$ on $\mathbb{H}^*$ are equivalent (with respect to $\mathrm{PSL}_2(\mathbb{Z})$) to

(a) ∞ (parabolic); $\Gamma_\infty = < \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} > \cong \mathbb{Z}$,

(b) i (elliptic); $\Gamma_i = < \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} > \cong \mathbb{Z}/2\mathbb{Z}$,

(c) $\rho := e^{\frac{2\pi i}{3}}$ (elliptic); $\Gamma_\rho = < \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} > \cong \mathbb{Z}/3\mathbb{Z}$.

Proof. Ad (a): This has already been proven.
Ad (b), (c): Let $z \in \mathbb{H}$ be a fixed point of $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, $\gamma \neq \mathrm{id}$. Since z is not a cusp we have

$$\frac{az+b}{cz+d} = z \Longleftrightarrow cz^2 + (d-a)z - b = 0,$$

and therefore get the solutions

$$z_{1,2} = \frac{a-d \pm \sqrt{(a-d)^2 - 4b}}{2c} = \frac{a-d \pm \sqrt{(a+d)^2 - 4}}{2c}.$$

Since z_1 or z_2 lies in $\mathbb{H}$ we have $|tr(\gamma)| = |a+d| < 2$. Together with the fact that $a+d \in \mathbb{Z}$, we get $tr(\gamma) \in \{-1, 0, 1\}$. Thus we could have the following three characteristic polynomials for γ: $\lambda^2 + 1$, $\lambda^2 + \lambda + +1$, $\lambda^2 - \lambda + 1$. Therefore we only have to consider γ's which satisfy ($\gamma \in \mathrm{SL}_2(\mathbb{Z})$)

$$\gamma^4 = \mathrm{id}\ (\gamma^2 \neq id),\ \gamma^3 = id,\ \gamma^3 = -id.$$

We start by considering the first equation (which will lead to (b)).

Assume $\gamma^4 = id$: Consider the polynomial ring $\mathbb{Z}[\gamma] \cong \mathbb{Z}[i]$.
The $\mathbb{Z}[i]$-module $\mathbb{Z}^2$ is torsion free. To see this let $0 \neq a + ib \in \mathbb{Z}[i]$, $x \in \mathbb{Z}^2$. Then $(a+ib)x = 0$ implies $(a^2+b^2)x = 0$. Hence $x = 0$.
Therefore the $\mathbb{Z}[i]$-modul $\mathbb{Z}^2$ is free of rank 1 and there exists $u \in \mathbb{Z}^2$ such that $\mathbb{Z}[i].u = \mathbb{Z}^2$. Hence u and $v := \gamma u$ together are a $\mathbb{Z}$-basis of $\mathbb{Z}^2$. Since $\gamma^2 = -id$ we have $\gamma[u, v] = [u, v]\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

If $\det([u, v]) = 1$, then γ is conjugate to $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$.

If $\det([u, v]) = -1$, then γ is conjugate to $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$.
Therefore every elliptic fixed point z of order 2 is equivalent to i and $\Gamma_i = < \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} >$. The other cases are left as an exercise. ∎

We consider the following situation: For $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ a subgroup of finite index, we have the following commutative diagram:

$$\begin{tikzcd} \mathbb{H}^* \arrow[r, "\mathrm{id}"] \arrow[d, "\pi_\Gamma"] & \mathbb{H}^* \arrow[d, "\pi_{\mathrm{PSL}_2(\mathbb{Z})}"] \\ \Gamma\backslash\mathbb{H}^* \arrow[r, "\pi_{\Gamma,\mathrm{PSL}_2(\mathbb{Z})}"] & \mathrm{PSL}_2(\mathbb{Z})\backslash\mathbb{H}^* \end{tikzcd}$$

Recall that a point $\pi_\Gamma(z) \in \Gamma\backslash\mathbb{H}^*$ ($z \in \mathbb{H}^*$) is called fixed point (with respect to Γ), if z has a non-trivial stabilizer group Γ_z. Note that this notion is well-defined, since the cardinality of the stabilizer group is invariant under conjugation.

Definition 2.9. The *ramification index* $e_{\pi_\Gamma(z)}$ of a point $\pi_\Gamma(z) \in \Gamma\backslash\mathbb{H}^*$ is defined as

$$e_{\pi_\Gamma(z)} := [\mathrm{PSL}_2(\mathbb{Z})_z : \Gamma_z].$$

A point $\pi_\Gamma(z) \in \Gamma\backslash\mathbb{H}^*$ is called *ramification point (with respect to $\pi_{\Gamma,\mathrm{PSL}_2(\mathbb{Z})}$)*, if $e_{\pi_\Gamma(z)} > 1$.

Proposition 2.10. Let $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ be a subgroup of finite index. Let

$$\pi_\Gamma(z_1), \ldots, \pi_\Gamma(z_r) \in \Gamma\backslash\mathbb{H}^*$$

denote the preimages of a point $\pi_{\mathrm{PSL}_2(\mathbb{Z})}(z) \in \mathrm{PSL}_2(\mathbb{Z})\backslash\mathbb{H}^*$. Then, the following assertions hold:

(a) The point $\pi_\Gamma(z_j)$ ($j = 1, \ldots, r$) can only be a fixed point, if $\pi_{\mathrm{PSL}_2(\mathbb{Z})}(z)$ is a fixed point. Hence, the fixed points of $\Gamma\backslash\mathbb{H}^*$ lie all above

$$\pi_{\mathrm{PSL}_2(\mathbb{Z})}(i), \pi_{\mathrm{PSL}_2(\mathbb{Z})}(\rho), \pi_{\mathrm{PSL}_2(\mathbb{Z})}(\infty).$$

(b) We have

$$\sum_{j=1}^{r} e_{\pi_\Gamma}(z_j) = [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma] =: N.$$

Proof. The first assertion of (a) follows immediately from $\Gamma_z \subseteq \mathrm{PSL}_2(\mathbb{Z})_z$. The second assertion of (a) follows from Proposition 2.8.
To prove (b), we recall how one obtains the points $\pi_\Gamma(z_j)$ ($j = 1, \ldots, r$) from the point $\pi_{\mathrm{PSL}_2(\mathbb{Z})}(z)$: We start with the decomposition

$$\bigcup_{k=1}^{N} \Gamma\gamma_k = \mathrm{PSL}_2(\mathbb{Z}),$$

which exists, since $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ is of finite index N. From this we obtain an orbit decomposition of the form

$$\pi_{\mathrm{PSL}_2(\mathbb{Z})}(z) = \mathrm{PSL}_2(\mathbb{Z})z = \bigcup_{k=1}^{N} \Gamma\gamma_k z.$$

Now we order the γ_k's in such a way that the first $r \leq N$ orbits represent exactly all pairwise disjoint orbits, i.e. we have a disjoint union

$$\pi_{\mathrm{PSL}_2(\mathbb{Z})}(z) = \dot{\bigcup}_{j=1}^{r} \pi_\Gamma(z_j),$$

where we have set $z_j := \gamma_j z$. We now prove that for $j = 1, \dots, r$, we have the identity

$$e_{\pi_\Gamma(z_j)} = \#\{\gamma_k \,|\, \Gamma\gamma_k z = \Gamma\gamma_j z\,, \text{i.e., } \Gamma z_k = \Gamma z_j\}.$$

We have

$$\begin{aligned}\#\{\gamma_k \,|\, \Gamma\gamma_k z = \Gamma\gamma_j z\} &= \#\{\gamma_k \,|\, \exists\gamma \in \Gamma : \gamma\gamma_k\gamma_j^{-1} z_j = z_j\} \\ &= |\mathrm{PSL}_2(\mathbb{Z})_{z_j} / \Gamma \cap \mathrm{PSL}_2(\mathbb{Z})_{z_j}| \\ &= [\mathrm{PSL}_2(\mathbb{Z})_{z_j} : \Gamma_{z_j}] = e_{\pi_\Gamma}(z_j).\end{aligned}$$

All in all, this yields

$$N = [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma] = \sum_{j=1}^{r} e_{\pi_\Gamma}(z_j),$$

as asserted. ∎

Digression. *(The genus of a Riemann surface)*
Let X be a compact Riemann surface. From topology we know that such 2-dimensional real, oriented, closed surfaces can be given the structure of a $4g$-gon :

$$a_1 b_1 a_1^{-1} b_1^{-1} \dots a_g b_g a_g^{-1} b_g^{-1}$$

(see for example: Seifert, Lehrbuch der Topologie, pp. 130 –142).
The number $g \in \mathbb{N}$ is the homeomorphy type of X, called genus of X. The genus g can also be computed with the help op a triangulation of X. Let

$$\begin{aligned}&E : \#\text{ 0-simplices (vertices)},\\ &K : \#\text{ 1-simplices (edges)},\\ &F : \#\text{ 2-simplices (areas)}.\end{aligned}$$

Then, we have the Euler polyeder formula

$$2 - 2g = E - K + F.$$

The genus can also be computed in terms of Betti numbers.

Proposition 2.11. Let $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ be a subgroup of finite index and let $X(\Gamma) := \Gamma\backslash\mathbb{H}^*$. Further let

$$\begin{aligned}N &:= [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma],\\ v_2 &:= \#\text{ of fixed points of order 2 of } X(\Gamma),\\ v_3 &:= \#\text{ of fixed points of order 3 of } X(\Gamma),\\ v_\infty &:= \#\text{ of cusps of } X(\Gamma).\end{aligned}$$

Then, the genus $g := g(X(\Gamma))$ of $X(\Gamma)$ is given by

$$g = 1 + \frac{N}{12} - \frac{v_2}{4} - \frac{v_3}{3} - \frac{v_\infty}{2}.$$

Proof. We start by considering the covering map

$$X(\Gamma) = \Gamma\backslash\mathbb{H}^* \overset{\pi_{\Gamma,\mathrm{PSL}_2(\mathbb{Z})}}{\longrightarrow} \mathrm{PSL}_2(\mathbb{Z})\backslash\mathbb{H}^* \cong \mathbb{P}^1(\mathbb{C})$$

Assume that the ramification points of $X(\Gamma)$ lie over the points

$$\mathbb{P}^1(\mathbb{C}) \ni x_j \qquad (j = 1, \ldots, h)$$

and denote these (for the moment) by

$$\xi_{jk} \qquad (j = 1, \ldots, h; k = 1, \ldots, r_j),$$

see also the picture given in the lecture. Starting from the preimages of a point

$$x_0 \in \mathbb{P}^1(\mathbb{C}), x_0 \neq x_j \, (j = 1, \ldots, h),$$

we perform disjoints cuts from

$$\pi^{-1}_{\Gamma,\mathrm{PSL}_2(\mathbb{Z})}(x_0) \text{ to } \xi_{jk}$$

in every sheet. Thereby, the Riemann surface $X(\Gamma)$ decomposes into $F = N$ copies of $\mathbb{P}^1(\mathbb{C})$, and we have performed $K = N \cdot h$ cuts. Finally, since there are N points lying over x_0, we have

$$E = N + \sum_{j=1}^{h} r_j.$$

Applying the Euler polyeder formula, we thus get

$$\begin{aligned} 2 - 2g &= E - K + F \\ &= (N + \sum_{j=1}^{h} r_j) - (N \cdot h) + N \\ &= 2N - \sum_{j=1}^{h} (N - r_j). \end{aligned}$$

Let now $e(\xi_{jk})$ denote the ramification orders of the points ξ_{jk}. Then, applying Proposition 2.10 (b), we compute (for $j = 1, \ldots, h$)

$$\sum_{k=1}^{r_j} (e(\xi_{jk}) - 1) = N - r_j.$$

Therefore, for the genus g of $X(\Gamma)$, we get the following formula

$$\begin{aligned} g &= 1 - N + \frac{1}{2} \sum_{j=1}^{h} (N - r_j) \\ &= 1 - N + \frac{1}{2} \sum_{j=1}^{h} \sum_{k=1}^{r_j} (e(\xi_{jk}) - 1). \end{aligned} \tag{2.1}$$

■

Lemma 2.12. Let $\pi_\Gamma(z_1), \ldots, \pi_\Gamma(z_r) \in \Gamma\backslash\mathbb{H}^*$ be the points lying over a point $\pi_{\mathrm{PSL}_2(\mathbb{Z})}(z) \in \mathrm{PSL}_2(\mathbb{Z})\backslash\mathbb{H}^*$. If Γ is a normal subgroup of $\mathrm{PSL}_2(\mathbb{Z})$, we have the identity

$$e_{\pi_\Gamma}(z_j) = e_{\pi_\Gamma}(z_1)$$

for $j = 1, \ldots, r$.

Proof. The group $\mathrm{PSL}_2(\mathbb{Z})/\Gamma$ acts on $\{\pi_\Gamma(z_1), \dots, \pi_\Gamma(z_r)\}$. Therefore

$$\begin{aligned} e_{\pi_\Gamma}(z_j) &= |\mathrm{Stab}_{\mathrm{PSL}_2(\mathbb{Z})/\Gamma}(\pi_\Gamma(z_j))| \\ &= |\mathrm{Stab}_{\mathrm{PSL}_2(\mathbb{Z})/\Gamma}(\pi_\Gamma(z_1))| = e_{\pi_\Gamma}(z_1). \end{aligned}$$

∎

Remark. Let $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ be a normal subgroup, as in the Lemma before. The points lying above $\pi_\Gamma(i)$ (resp. $\pi_\Gamma(\rho)$) are either all of order 2 (resp. 3) or all of order 1, i.e. no fixed points.

2.2 Congruence groups

We now discuss some examples of congruence groups.

Definition 2.13. Let $N \in \mathbb{N}$, $N \geq 1$. We define the subgroup

$$\Gamma(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, a \equiv d \equiv 1 \mod N\,,\ b \equiv c \equiv 0 \mod N \right\}.$$

The group $\overline{\Gamma(N)} := \Gamma(N)/\{\pm \mathrm{id}\} \subseteq \mathrm{PSL}_2(\mathbb{Z})$ is called *principle congruence subgroup of level N*.

Note that $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ and $\overline{\Gamma(1)} = \mathrm{PSL}_2(\mathbb{Z})$.

Lemma 2.14. For the index of the principle congruence $\overline{\Gamma(N)}$ in $\mathrm{PSL}_2(\mathbb{Z})$, we have

$$[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma(N)}] = \begin{cases} \frac{N^3}{2} \prod\limits_{p \mid N} (1 - p^{-2}), & \text{if } N > 2; \\ 6, & \text{if } N = 2. \end{cases}$$

Proof. We first observe that following short sequence

$$1 \longrightarrow \Gamma(N) \longrightarrow \mathrm{SL}_2(\mathbb{Z}) \xrightarrow{f} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow 1$$

is exact, which yields

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

To prove this claim, it remains to show that f is surjective. Let $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. We have to find $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \mod N$. We know $(\alpha, \beta, N) = 1$, hence we can find $\beta' \in \mathbb{Z}$ with $(\alpha, \beta + \beta' N) = 1$. Therefore, we can assume without loss of generality that $(\alpha, \beta) = 1$. Now, we can choose $\gamma', \delta' \in \mathbb{Z}$ such that

$$\alpha\delta' - \beta\gamma' = 1.$$

We then set

$$\begin{aligned} a &:= \alpha, \\ b &:= \beta, \\ c &:= \gamma + \gamma'(1 - \alpha\delta + \beta\gamma), \\ d &:= \delta + \delta'(1 - \alpha\delta + \beta\gamma). \end{aligned}$$

Then one easily verifies that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ satisfies the required properties.

Let $N = \prod_p p^{\lambda_p}$ be the prime factorization of N. Then, we have

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})| = \prod_{p\,|N} |\mathrm{SL}_2(\mathbb{Z}/p^{\lambda_p}\mathbb{Z})|.$$

To compute the orders $|\mathrm{SL}_2(\mathbb{Z}/p^{\lambda_p}\mathbb{Z})|$, we observe that

$$|\mathrm{SL}_2(\mathbb{Z}/p^{\lambda_p}\mathbb{Z})| = \frac{|\mathrm{GL}_2(\mathbb{Z}/p^{\lambda_p}\mathbb{Z})|}{p^{\lambda_p} - p^{\lambda_p - 1}} = \frac{|\mathrm{GL}_2(\mathbb{Z}/p^{\lambda_p}\mathbb{Z})|}{p^{\lambda_p}(1 - p^{-1})},$$

and we employ well-known facts for the general linear group, namely

$$\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) = (p^2 - 1)(p^2 - p).$$

We now consider the exact sequence

$$1 \longrightarrow \ker(f') \longrightarrow \mathrm{GL}_2(\mathbb{Z}/p^{\lambda_p}\mathbb{Z}) \xrightarrow{f'} \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow 1.$$

Since $\ker(f')$ consists of the elements in $M_2(\mathbb{Z}/p^{\lambda_p}\mathbb{Z})$ which are congruent to the identity matrix modulo p, we find easily find that

$$|\ker(f')| = p^{4(\lambda_p - 1)}.$$

All in all, we get

$$\begin{aligned} |\mathrm{SL}_2(\mathbb{Z}/p^{\lambda_p}\mathbb{Z})| &= \frac{p^{4(\lambda_p - 1)} \cdot (p^2 - 1)(p^2 - p)}{p^{\lambda_p}(1 - p^{-1})} \\ &= p^{3\lambda_p}(1 - p^{-2}). \end{aligned}$$

Hence, we obtain

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p\,|N} (1 - p^{-2}).$$

Finally, observing that $-1 \in \Gamma(N)$ if and only if $N = 2$, the claimed formula follows. ■

Lemma 2.15. Let $N > 1$ and $X(\overline{\Gamma(N)}) = \overline{\Gamma(N)} \backslash \mathbb{H}^*$. Then

(a)

$$v_\infty = \frac{[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma(N)}]}{N} = \begin{cases} \frac{N^2}{2} \prod\limits_{p\,|N} (1 - p^{-2}), & \text{if } N > 2; \\ 3, & \text{if } N = 2. \end{cases}$$

(b)

$$v_2 = v_3 = 0.$$

Proof. (a) Since $\overline{\Gamma(N)}$ is a normal subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ the ramification orders of all cusps of $X(\overline{\Gamma(N)})$ are equal (by Lemma 2.12) say equal to e. We first notice that

$$\overline{\Gamma(N)}_\infty = < \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} > .$$

Hence

$$e = [\mathrm{PSL}_2(\mathbb{Z})_\infty : \overline{\Gamma(N)}_\infty] = N$$

and, since $v_\infty e = [\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma(N)}]$, we have $v_\infty = [\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma(N)}]/N$. Together with the last lemma the claim follows.
(b) Since $\overline{\Gamma(N)}$ is a normal subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ we only have to consider the elliptic fixed points $\pi_{\overline{\Gamma(N)}}(i)$ and $\pi_{\overline{\Gamma(N)}}(\rho)$.
We have

$$\mathrm{PSL}_2(\mathbb{Z})_i = < \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} > , \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \notin \Gamma(N).$$

Hence $\overline{\Gamma(N)}_i$ is trivial for all $N > 1$. Therefore $v_2 = 0$. The proof of $v_3 = 0$ is analogous. ∎

Corollary 2.16. For $N > 1$, the genus g of $X(\overline{\Gamma(N)})$ is given by

$$g = 1 + \frac{[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma(N)}]}{12N}(N-6) = 1 + \frac{v_\infty}{12}(N-6).$$

Proof. Using the formula given in Proposition 2.11, we get

$$g = 1 + \frac{[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma(N)}]}{12} - \frac{v_2}{4} - \frac{v_3}{3} - \frac{v_\infty}{2} = 1 + \frac{[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma(N)}]}{12} - \frac{[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma(N)}]}{2N},$$

which yields the claim. ∎

▪ **Example 2.17.** The Riemann surface $X(\overline{\Gamma(2)})$ has $6/2 = 3$ cusps, which can be represented by $\infty = [1:0]$, $0 = [0:1]$, and $1 = [1:1]$. Thus, we have $g(\overline{\Gamma(2)}) = 0$. See the lecture for a picture of a fundamental domain, or, e.g., the book of Katok.
One can show, that the genus of $X(\overline{\Gamma(N)})$ is zero, if and only if $N = 1, 2, 3, 4, 5$. ▪

Definition 2.18. A subgroup $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ is called *congruence subgroup* of $\mathrm{PSL}_2(\mathbb{Z})$, if $\overline{\Gamma}(N) \subseteq \Gamma$ for some $N \in \mathbb{N}$. The *level* of a congruence subgroup Γ is the smallest such N. (Note that from this definition it immediately follows that congruence groups are examples for groups of finite index in $\mathrm{PSL}_2(\mathbb{Z})$.)

Remark. The literature on congruence subgroups is vast, and the subject remains very active. Rademacher conjectured that there are only finitely many genus 0 congruence subgroups. Stronger versions of the conjecture were proved by Thompson, and Cox and Parry, which show that the number of congruence subgroups of any genus is finite.

Definition 2.19. Let $N \in \mathbb{N}$. We define

$$\Gamma_0(N) = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \mod N \}$$

and $\overline{\Gamma_0(N)} := \Gamma_0(N)/\{\pm \mathrm{id}\}$; it is is called *Hecke congruence group of level N*.

Lemma 2.20. For the index of the congruence $\overline{\Gamma_0(N)}$ in $\mathrm{PSL}_2(\mathbb{Z})$, we have

$$[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma_0(N)}] = N \prod_{p \mid N} (1 + p^{-1}).$$

Proof. This proof is left as exercise. For completeness, we give the idea of proof. We consider the map f as in the proof of Lemma for $\Gamma(N)$. Considering the image of $\Gamma_0(N)$ under f, we get

$$\Gamma_0(N)/\Gamma(N) \cong \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \right\}.$$

Hence, we get

$$[\Gamma_0(N):\Gamma(N)] = N\varphi(N) = N^2\prod_{p\,|N}(1-p^{-1}).$$

Since $-\mathrm{id}\in\Gamma_0(N)$, we have

$$\begin{aligned}[\mathrm{PSL}_2(\mathbb{Z}):\overline{\Gamma_0(N)}] &= [\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(N)] = \frac{[\mathrm{SL}_2(\mathbb{Z}):\Gamma(N)]}{[\Gamma_0(N):\Gamma(N)]}\\ &= \frac{N^3\prod_{p\,|N}(1-p^{-2})}{N^2\prod_{p\,|N}(1-p^{-1})} = N\prod_{p\,|N}(1+p^{-1}).\end{aligned}$$

■

Remark. *(Legendre symbol/quadratic residue symbol)* Let p be an odd prime number. We define

$$\left(\frac{n}{p}\right) = \begin{cases}1 & p\not|\,n\ \wedge\ x^2\equiv n \mod p \text{ is solvable in } \mathbb{Z}\\ -1 & p\not|\,n\ \wedge\ x^2\equiv n \mod p \text{ is not solvable in } \mathbb{Z}\\ 0 & p\,|\,n\end{cases}$$

If $p=2$ we define

$$\left(\frac{n}{2}\right) = \begin{cases}1 & n\equiv 1 \mod 8\\ -1 & n\equiv 5 \mod 8\\ 0 & \text{otherwise}\end{cases}$$

Lemma 2.21. For $X(\overline{\Gamma_0(N)}) = \overline{\Gamma_0(N)}\backslash\mathbb{H}^*$ we have

(a) $v_\infty = \sum_{\substack{d|\,N\\ d>0}}\varphi((d,\frac{N}{d}))$ with Euler's φ-function

(b) $v_2 = \begin{cases}0 & 4|\,N\\ \prod_{p|\,N}\left(1+\left(\frac{-1}{p}\right)\right) & \text{otherwise}\end{cases}$

(c) $v_3 = \begin{cases}0 & 9|\,N\\ \prod_{p|\,N}\left(1+\left(\frac{-3}{p}\right)\right) & \text{otherwise}\end{cases}$

with

$$\left(\frac{-1}{p}\right) = \begin{cases}1 & p\equiv 1 \mod 4\\ -1 & p\equiv 3 \mod 4\\ 0 & \text{otherwise}\end{cases}$$

and

$$\left(\frac{-3}{p}\right) = \begin{cases}1 & p\equiv 1 \mod 3\\ -1 & p\equiv 2 \mod 3\,.\\ 0 & \text{otherwise}\end{cases}$$

Proof. We will only prove the case where $N=p$ is an odd prime.

(a) In this case the two cusps $\pi_{\overline{\Gamma_0(p)}}(\infty)$ and $\pi_{\overline{\Gamma_0(p)}}(0)$ lie above $\pi_{\mathrm{PSL}_2(\mathbb{Z})}(\infty)$. For the ramification indices we compute

$$e(\pi_{\overline{\Gamma_\infty(p)}}(\infty)) = 1\ ,\ \ \pi_{\overline{\Gamma_0(p)}}(0) = p.$$

Since their sum is $p+1=\mu_p^0$ we conclude $v_\infty = 2$, as asserted.

(b) We have to study how the $\mathrm{SL}_2(\mathbb{Z})$ conjugation class S_1 of $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (resp. the conjugation class S_2 of $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$) splits into $\Gamma_0(p)$ conjugation classes.

To do this let, let $\Lambda := \mathbb{Z}^2$, $\Lambda_p := \mathbb{Z} \oplus p\mathbb{Z}$. If $\sigma \in S_1$ (resp. $\sigma \in S_2$) then $\mathbb{Z}[\sigma] \cong \mathbb{Z}[i]$, hence Λ is a free $\mathbb{Z}[\sigma]$-module of rank 1. Therefore there exists a $\mathbb{Z}$-linear isomorphism $f_\sigma : \mathbb{Z}[i] \longrightarrow \Lambda$.
For the submodule $\Lambda_p \subset \Lambda$ we define $a_\sigma := f_\sigma^{-1}(\Lambda_p) \subseteq \mathbb{Z}[i]$.
Then

$$a_\sigma \subseteq \mathbb{Z}[i] \text{ ideal} \Longleftrightarrow \sigma \in S_1 \cap \Gamma_0(p) \text{ (resp. } \sigma \in S_2 \cap \Gamma_0(p)).$$

Since

$$\mathbb{Z}[i]/a_\sigma \cong \Lambda/\Lambda_p \cong \mathbb{Z}/p\mathbb{Z}$$

we get
(i) $N_{\mathbb{Q}(i)/\mathbb{Q}}(a_\sigma) = p$
(ii) $a_\sigma \notin \mathbb{Z}$.
Furthermore we have the following bijections :

$$\left\{ \Gamma_0(p)\text{-conjugacy classes of } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$
$$\cong \{a \subseteq \mathbb{Z}[i], \text{ideal} \mid N_{\mathbb{Q}(i)/\mathbb{Q}}(a_\sigma) = p\,,\, a_\sigma \notin \mathbb{Z}\}$$
$$\cong \{a \subseteq \mathbb{Z}[i], \text{prime ideal} \mid N_{\mathbb{Q}(i)/\mathbb{Q}}(a_\sigma) = p\,,\, p \text{ decomposes}\}$$

The cardinality of the last set equals 0, if $p \equiv 3 \mod 4$ and it is 2, if $p \equiv 1 \mod 4$. Thus we get

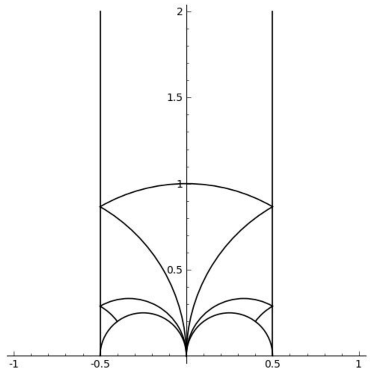
$$v_2 = 1 + \left(\frac{-1}{p}\right).$$

(c) Analogous to (b). ■

Corollary 2.22. The genus of $X(\overline{\Gamma_0(p)})$, if p is an odd prime, is given by

$$g = \frac{p+1}{12} - \frac{1}{4}\left(1 + \left(\frac{-1}{p}\right)\right) - \frac{1}{3}\left(1 + \left(\frac{-3}{p}\right)\right)$$

■ **Example 2.23.** The Riemann surface $X(\overline{\Gamma_0(4)})$ has 3 cusps, which can be represented by $\infty = [1:0]$, $0 = [0:1]$, and $1/2 = [1:2]$. Thus, we have $g(\overline{\Gamma(4)}) = 0$. Picture of a fundamental domain:



One can show, that Riemann surfaces of the form $X(\overline{\Gamma_0(N)})$, with genus 0 and no elliptic fixed points, are exactly the one with $N = 4, 6, 8, 9, 12, 16, 18$. ■

Remark. Article of Elstrodt on fundamental domains `https://arxiv.org/abs/2308.11997`.

Remark. Fundamental drawer by H. A. Verrill and I. Breeze

`https://www.mathamaze.co.uk/complexplane/`

Exercise 2.1 For $N \in \mathbb{N}$, $N > 1$, we consider the subgroup

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \mod N \right\}$$

of $\mathrm{SL}_2(\mathbb{Z})$. Let

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

and let p be a prime number. For $j \in \mathbb{N}$, $0 \le j \le p$, we set

$$\alpha_j := \begin{cases} ST^j, & \text{if } 0 \le j \le p-1; \\ E, & \text{if } j = p. \end{cases}$$

(a) Prove that

$$\mathrm{SL}_2(\mathbb{Z}) = \dot{\bigcup}_{j=0}^{p} \alpha_j^{-1}\Gamma_0(p) = \dot{\bigcup}_{j=0}^{p} \Gamma_0(p)\alpha_j.$$

(b) Using (a), conclude that there is a fundamental domain $\mathcal{F}_{\Gamma_0(p)}$ for $\Gamma_0(p)$ satisfying

$$\mathcal{F}_{\Gamma_0(p)} = \bigcup_{j=0}^{p} \alpha_j \mathcal{F}_{\mathrm{SL}_2(\mathbb{Z})}.$$

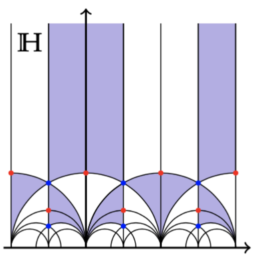
(c) Draw a fundamental domain $\mathcal{F}_{\Gamma_0(2)}$ and determine all the cusps of $\Gamma_0(2)$, i.e., the orbits $\Gamma_0(2)[r : s]$ with $[r : s] \in \mathbb{P}^1(\mathbb{Q})$.

■

Exercise 2.2 Determine the genus of the Riemann surface $X(\Gamma)$ for

$$\Gamma \in \left\{ \overline{\Gamma_0(2)}, \overline{\Gamma_0(4)}, \overline{\Gamma_0(11)} \right\}.$$

■



3. Modular forms for $\mathrm{SL}_2(\mathbb{Z})$

In this chapter, we let $\Gamma := \mathrm{SL}_2(\mathbb{Z})$.

Definition 3.1. A *modular function* (resp. a *modular form*) *of weight* $k \in \mathbb{Z}$ *for* $\mathrm{SL}_2(\mathbb{Z})$ is a function $f : \mathbb{H} \longrightarrow \mathbb{C}$ satisfying

(i) $f(\gamma z) = (cz+d)^k f(z)$ for any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathbb{H}$.

(ii) f is meromorphic (resp. holomorphic) on $\mathbb{H}$.

(iii) f is meromorphic (resp. holomorphic) at ∞, i.e., f has a Fourier expansion of the form

$$f(z) = \sum_{n=n_0}^{\infty} a_n q^n \tag{3.1}$$

for some $n_0 \in \mathbb{Z}$ (resp. $n_0 \in \mathbb{N}$), where $q := e^{2\pi i z}$ and with coefficients

$$a_n = \int_0^1 f(z) q^{-n} dz \in \mathbb{C}.$$

Definition 3.2. A *cusp form of weight* k *for* $\mathrm{SL}_2(\mathbb{Z})$ is a modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$, which vanishes at ∞, i.e., we have $n_0 > 0$ in (3.1), that is $a_0 = 0$.

Remark. Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, we have $f(z+1) = f(z)$ for all $z \in \mathbb{H}^*$ for a function that satisfies (i) and since

$$f(z) = \sum_{n<0} a_n q^n + a_0 + \sum_{n>0} a_n q^n,$$

where $a_n q^n = \mathcal{O}(e^{-2\pi n y})$, the starting index n_0 from (iii) tells us how a modular function f behaves at ∞.

Remark. (a) If k is odd, there are no modular functions $f \neq 0$ of weight k. Namely, applying (i) of Definition 3.1 with $\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we obtain the equality

$$f(z) = (0z-1)^k f(z) = (-1)^k f(z) = -f(z).$$

(b) To verify property (i) from Definition 3.1 it suffices to verify (i) for the generators

$$T := \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \quad S := \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$$

of $\mathrm{SL}_2(\mathbb{Z})$, i.e., it suffices to show that

$$f(z+1) = f(z), \quad f\left(-\frac{1}{z}\right) = f(z)$$

holds for all $z \in \mathbb{H}$.

(c) If $k=0$, then f is a well-defined function on $\Gamma\backslash\mathbb{H}$. If f is a modular form of weight $k=2$, then $f(z)dz$ defines a differential form on $\Gamma\backslash\mathbb{H}$, since then, we have

$$f(z)dz \stackrel{!}{=} f(\gamma z)d(\gamma z)$$

for all $\gamma \in \Gamma$.

Remark. The set

$$\begin{aligned}\mathcal{M}_k(\Gamma) &:= \{f \mid f \text{ is a modular form of weight } k \text{ for } \Gamma\}, \text{ resp.}\\ \mathcal{S}_k(\Gamma) &:= \{f \mid f \text{ is a cusp form of weight } k \text{ for } \Gamma\}\end{aligned}$$

is a $\mathbb{C}$-vector space. Functions in $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ resp. $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ are also called *modular forms* resp. *cusp forms of level* 1.

We now consider/define the following examples.

■ **Example 3.3.** (i) The constant functions are modular forms of weight 0 for Γ.

(ii) The normalized Eisenstein series $E_k(z) := G_k(z)/(2\zeta(k))$ of weight k ($k \in \mathbb{N}$, $k > 2$, k even) satisfies (cf. Definition 6.1)

$$\begin{aligned}E_k(z) &:= \frac{G_k(z)}{2\zeta(k)} = \frac{1}{2}\sum_{\substack{(m,n)\in\mathbb{Z}^2\\ (m,n)=1}} \frac{1}{(mz+n)^k}\\ &= 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n)\cdot q^n \qquad (3.2)\end{aligned}$$

with the Bernoulli numbers B_k (see Definition 6.7) and with (cf. (6.1))

$$\sigma_{k-1}(n) = \sum_{\substack{d|n\\ 1\le d\le n}} d^{k-1},$$

and is an element of $\mathcal{M}_k(\Gamma) \setminus \mathcal{S}_k(\Gamma)$. The last claim follows from Proposition 6.3 together with Proposition 6.6. The proof of expansion (3.2) will be given on the next pages. To explicitly determine the coefficients of the q-series for $E_4(z)$ and $E_6(z)$, note that $-8/B_4 = 240 = 2^4\cdot 3\cdot 5$ and $-12/B_6 = -504 = -2^3\cdot 3^2\cdot 7$.

(iii) The Δ-function, also called *discriminant modular form*, is defined by

$$\begin{aligned}\Delta(z) &:= \frac{E_4(z)^3 - E_6(z)^2}{1728} = q - 24q^2 + \dots \\ &=: \sum_{n=1}^{\infty} \tau(n) \cdot q^n,\end{aligned}$$

with the so-called Ramanujan τ function, and is an element of $\mathcal{S}_{12}(\Gamma)$. In 1947, Lehmer conjectured that $\tau(n) \neq 0$ for all $n \in \mathbb{N}_{>0}$. This assertion is also known as Lehmer's conjecture and it is still open today, even though it has been verified for all $n \in \mathbb{N}$ with $n < 816212624008487344127999$ (in the year 2013).

(iv) The j-function is defined by

$$\begin{aligned}j(z) &:= \frac{E_4(z)^3}{\Delta(z)} = 1728 \frac{E_4(z)^3}{E_4^3(z) - E_6^2(z)} \\ &= \frac{1}{q} + 744 + \dots\end{aligned} \tag{3.3}$$

and is a modular function for Γ of weight 0 (but not a modular form Γ). Note that we will later see that Δ has no zeros on $\mathbb{H}$.

■

Proof of expansion (3.2). By Proposition 6.6, we have (for $k \geq 4$ an even integer) the identity

$$G_k(z) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n$$

Hence, we get

$$E_k(z) = \frac{G_k(z)}{2\zeta(k)} = 1 + \frac{(2\pi)^k i^k \cdot k}{\zeta(k) k!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n.$$

Using (6.4) (with $2k$ replaced by k), namely

$$\zeta(k) = \frac{-(2\pi)^k i^k}{k!} \cdot \frac{B_k}{2}.$$

we get

$$E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n,$$

as asserted. ■

In the following, we will be interested in computing the dimension of the space of modular forms resp. cusp forms of weight k for Γ. In a first step, we prove the $\frac{k}{12}$-formula, also called valence formula, for Γ.

Definition 3.4. Let $f \neq 0$ be a modular function of weight k for Γ. For $z \in \mathbb{H}$, we define

$$\nu_z(f)$$

to be the order of the zero (respectively, minus the order of the pole) of $f(z)$ at z. By

$$v_\infty(f),$$

we denote the index of the first non-vanishing term in the q-series (3.1) of f.

Remark. (i) Since $(cz+d)^k$ has no zeros in $\mathbb{H}$, we have

$$v_{\gamma z}(f) = v_z(f)$$

for all $\gamma \in \Gamma$ and $z \in \mathbb{H}$.
(ii) For the functions given in Example 3.3, we have

$$\nu_\infty(E_k) = 0, \qquad \nu_\infty(\Delta) = 1, \qquad \nu_\infty(j) = -1.$$

Theorem 3.5 — $\frac{k}{12}$-formula, valence formula for $\mathrm{SL}_2(\mathbb{Z})$. Let $f \neq 0$ be a modular function of weight k for Γ. Then, we have

$$\nu_\infty(f) + \frac{\nu_i(f)}{2} + \frac{\nu_\rho(f)}{3} + \sum_{\substack{\Gamma z \in \Gamma\backslash\mathbb{H} \\ z \notin \Gamma i, \Gamma\rho}} \nu_z(f) = \frac{k}{12}, \tag{3.4}$$

where $\rho := e^{2\pi i/3}$.

Proof. The idea of proof is to count the zeros and poles of f in $\Gamma\backslash\mathbb{H}$ by integrating the logarithmic derivative of f along the boundary of a (standard) fundamental domain $\mathcal{F}_\Gamma$. The proof is conducted in four steps.

1. step: We choose $T > 0$ in such a way that T is greater than the imaginary part of any zero or pole of f in $\mathbb{H}$. This is possible, since after a change of coordinates $z \mapsto q$, the function $\tilde{f} = f(q)$ is a meromorphic function in a disc about $q = 0$.

picture

2. step: We cut the fundamental domain $\mathcal{F}_\Gamma$ at height T and obtain $\mathcal{F}_\Gamma^T := \mathcal{F}_\Gamma \cap \{\mathrm{Im}(z) \leq T\}$. We then choose a closed path $\mathcal{C}$ along the boundary of $\mathcal{F}_\Gamma^T$ in such a way (see picture!) that every zero and every pole of f lying on the boundary of $\mathcal{F}_\Gamma^T$ is avoided by the segment of a circle of radius $\varepsilon > 0$ (ε small) and every Γ-equivalence class of a zero or a pole of f is contained exactly once inside of $\mathcal{C}$, and such that, if Γi or $\Gamma\rho$ contain zeros or poles of f, they lie outside of $\mathcal{C}$.

picture with $\mathcal{C}_1$ up to $\mathcal{C}_8$

By the residue theorem, we then have

$$\sum_{\substack{\Gamma z \in \Gamma\backslash\mathbb{H} \\ z \notin \Gamma i, \Gamma\varrho}} \nu_z(f) = \frac{1}{2\pi i} \int_{\mathcal{C}} \frac{f'(z)}{f(z)} dz = \frac{1}{2\pi i} \lim_{\varepsilon \to 0} I_\varepsilon,$$

where we have set

$$I_\varepsilon := \sum_{j=1}^{8} I_j$$

with

$$I_j := \int_{\mathcal{C}_j} \frac{f'(z)}{f(z)} dz.$$

3. step: We now consider step by step the integrals I_j. First of all, we have

$$I_7 = \int\limits_{\mathcal{C}_7} \frac{f'(w)}{f(w)} dw = \int\limits_{-\mathcal{C}_1} \frac{f'(z-1)}{f(z-1)} dz = -I_1,$$

where we substituted $z := w + 1$ in the first equality, and made use of $f(z-1) = f(z)$ and $f'(z-1) = f'(z)$ for the second equality. Next, we compute

$$I_5 = \int\limits_{\mathcal{C}_5} \frac{f'(w)}{f(w)} dw = \int\limits_{-\mathcal{C}_3} \frac{f'(-\frac{1}{z})}{f(-\frac{1}{z})} d(-\frac{1}{z}) = -I_3 + k \cdot \int\limits_{-\mathcal{C}_3} \frac{dz}{z},$$

where we substituted $w := -\frac{1}{z}$ in the first equality, and made use of

$$\begin{aligned} d\Big(-\frac{1}{z}\Big) &= \frac{dz}{z^2}, \\ f\Big(-\frac{1}{z}\Big) &= z^k f(z), \\ f'\Big(-\frac{1}{z}\Big)\frac{1}{z^2} &= kz^{k-1} f(z) + z^k f'(z) \end{aligned}$$

for the second equality. Furthermore, we get

$$\frac{1}{2\pi i} I_8 = \frac{1}{2\pi i} \int\limits_{\mathcal{C}_8} \frac{f'(z)}{f(z)} dz = \frac{1}{2\pi i} \oint\limits_{\text{circle around 0 of radius } e^{-2\pi T}} \frac{\tilde{f}'(q)}{\tilde{f}(q)} dq = -\nu_\infty(f),$$

with

$$f(z) = \sum_{n=n_0}^{\infty} a_n q^n =: \tilde{f}(q).$$

Finally, to compute I_2, resp. I_4, resp. I_6, we employ the formula

$$\frac{1}{2\pi i} \int_{\substack{\text{segment of a circle} \\ \text{around } w \text{ of angle } \vartheta}} \frac{f'(z)}{f(z)} dz \to -\frac{\vartheta}{2\pi} \nu_z(f),$$

as $\varepsilon \to 0$, with $w = \rho$, $\vartheta = \frac{2\pi}{6}$, resp. $w = i$, $\vartheta = \pi$, resp. $w = -\frac{1}{\rho}$, $\vartheta = \frac{2\pi}{6}$.

4. step: Adding up the results obtain in step 3, yields

$$\frac{1}{2\pi i} \lim_{\varepsilon \to 0} I_\varepsilon = \frac{k}{2\pi i} \Big(\lim_{\varepsilon \to 0} \int\limits_{-\mathcal{C}_3} \frac{dz}{z} \Big) - \nu_\infty(f) - \frac{1}{6}\nu_\varrho(f) - \frac{1}{2}\nu_i(f) - \frac{1}{6}\nu_{-1/\varrho}(f)$$

After substituting $z := e^{ir}$, we get the equality

$$\lim_{\varepsilon \to 0} \int\limits_{-\mathcal{C}_3} \frac{dz}{z} = i \int\limits_{\frac{\pi}{2}}^{\frac{2\pi}{3}} dr = \frac{\pi i}{6}.$$

Also, by Remark 3, we have $\nu_{-1/\varrho}(f) = \nu_\varrho(f)$. All in all, we thus get

$$\frac{1}{2\pi i} \lim_{\varepsilon \to 0} I_\varepsilon = \frac{k}{12} - \nu_\infty(f) - \frac{\nu_i(f)}{2} - \frac{\nu_\varrho(f)}{3},$$

which proves the claim. ∎

Remark. Since $\nu_\infty(\Delta) = 1$ and $\Delta \in \mathcal{S}_{12}(\mathrm{SL}_2(\mathbb{Z}))$, we deduce from (3.4) the identity

$$1 + \frac{\nu_i(f)}{2} + \frac{\nu_\rho(f)}{3} + \sum_{\substack{\Gamma z \in \Gamma\backslash\mathbb{H} \\ z \notin \Gamma i, \Gamma\rho}} \nu_z(f) = 1.$$

Hence, Δ has no zeros on $\mathbb{H}$.
We now will apply the $k/12$-formula to obtain dimension formulas for $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ and $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$.

Lemma 3.6. Let $\Gamma := \mathrm{SL}_2(\mathbb{Z})$. For $k \in \mathbb{Z}$, k even, we have:
(i) $\mathcal{M}_k(\Gamma) = \{0\}$ for $k < 0$.
(ii) $\mathcal{M}_0(\Gamma) = \mathbb{C}$.
(iii) $\mathcal{M}_2(\Gamma) = \{0\}$,
(iv) $\mathcal{M}_k(\Gamma) = \mathbb{C} \cdot E_k$ for $k = 4, 6, 8, 10, 14$.
(v) $\mathcal{S}_k(\Gamma) = \{0\}$ for $k = 4, 6, 8, 10, 14$.

Proof. (i) The left hand side of the $\frac{k}{12}$-formula (3.4) consists of non-negative terms, whereas right hand side of (3.4) is negative for $k < 0$. This proves (i).
(ii) Let $f \in M_0(\Gamma)$ and let c be a value of f. Then the function $f - c \in \mathcal{M}_0(\Gamma)$ has a zero. Hence the LHS of (3.4) is positive, but the RHS of (3.4) equals zero for $k = 0$. Hence $f - c \equiv 0$, that is, $f(z) = c$ for all $z \in \mathbb{H}$.
(iii) This claim follows, since

$$\alpha + \frac{\beta}{2} + \frac{\gamma}{2} = \frac{1}{6}$$

has no solution for $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}$.
(iv) Let $f \in \mathcal{M}_k(\Gamma)$, $f \neq 0$. We have the following table (easy exercise):

k	$\frac{k}{12}$	$\nu_{i\infty}(f)$	$\nu_i(f)$	$\nu_\varrho(f)$
4	$\frac{1}{3}$	0	0	1
6	$\frac{1}{2}$	0	1	0
8	$\frac{2}{3}$	0	0	2
10	$\frac{5}{6}$	0	1	1
14	$\frac{7}{6}$	0	1	2

Hence f and E_k have the same zeros and therefore

$$\frac{f(z)}{E_k(z)} \in \mathcal{M}_0(\Gamma).$$

From (ii), we thus conclude that

$$\frac{f(z)}{E_k(z)} = c$$

for a constant $c \in \mathbb{C}$. This proves (iv).
(v) For $k = 4, 6, 8, 10, 14$ the claim follows from the table in (iv).

■

Proposition 3.7. For $k \in \mathbb{N}$, k even, we have:
(i) $\mathcal{S}_k(\Gamma) = \Delta \cdot \mathcal{M}_{k-12}(\Gamma)$, if $k \geq 12$. In particular, we have $\mathcal{S}_{12}(\Gamma) = \mathbb{C} \cdot \Delta$.
(ii) $\mathcal{M}_k(\Gamma) = \mathbb{C} \cdot E_k \oplus \mathcal{S}_k(\Gamma)$ if $k > 2$.

Proof. (a) Let $k \geq 12$ be even and let $f \in \mathcal{S}_k(\Gamma)$, hence $v_\infty(f) \geq 1$. Since Δ has no zeros on $\mathbb{H}$ (by the table in (iv) above, see also the remark above) we conclude

$$\frac{f(z)}{\Delta(z)} \in \mathcal{M}_{k-12}(\Gamma).$$

This proves the claim. For $k = 12$, we use that $\mathcal{M}_0(\Gamma) = \mathbb{C}$.

(b) Let $k > 2$ be even and let $f \in \mathcal{M}_k(\Gamma)$. Then there exists a constant c (more precisely, $c = a_0(f)$, where $f = \sum_{n=0}^{\infty} a_n(f)q^n$ is the Fourier expansion of f) with

$$f - c \cdot E_k \in \mathcal{S}_k(\Gamma).$$

This proves the claim. ■

Remark. Using the above results, on can easily compute $\dim_{\mathbb{C}} \mathcal{M}_k(\Gamma)$ for $k = 0, 2, 4, \ldots, 14$.

k	0	2	4	6	8	10	12	14
$\dim_{\mathbb{C}} \mathcal{M}_k(\Gamma)$	1	0	1	1	1	1	2	1

Theorem 3.8 For $k \in \mathbb{N}$, k even, we have:

$$\dim_{\mathbb{C}} \mathcal{M}_k(\Gamma) = \begin{cases} \left[\frac{k}{12}\right], & \text{if } k \equiv 2 \mod 12; \\ \left[\frac{k}{12}\right] + 1, & \text{if } k \not\equiv 2 \mod 12. \end{cases}$$

Proof. By Lemma 3.6 and Proposition 3.7 the assertion is true for $0 \leq k \leq 14$, k even. We already know that
(i) $\dim_{\mathbb{C}} \mathcal{M}_k(\Gamma) = 1 + \dim_{\mathbb{C}} \mathcal{S}_k(\Gamma)$ for $k > 2$, k even.
(ii) $\dim_{\mathbb{C}} \mathcal{S}_k(\Gamma) = \dim_{\mathbb{C}} \mathcal{M}_{k-12}(\Gamma)$ for $k \geq 12$, k even.
Hence for $k \geq 12$, k even, it holds that

$$\dim_{\mathbb{C}} \mathcal{M}_k(\Gamma) = 1 + \dim_{\mathbb{C}} \mathcal{M}_{k-12}(\Gamma)$$

The claim follows from induction on k (exercise). ■

Theorem 3.9 Let $k \in \mathbb{N}$, $k > 2$ be even and let $f \in \mathcal{M}_k(\Gamma)$. Then, we can write

$$f(z) = \sum_{a,b \in \mathbb{N}} c_{a,b} \cdot E_4(z)^a \cdot E_6(z)^b$$

for certain constants $c_{a,b} \in \mathbb{C}$.

Proof. To ease notation, we write $\mathcal{M}_k := \mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k := \mathcal{M}_k(\Gamma)$. For $k = 4, 6, 8, 10, 14$, we observe that

$$E_4 \in \mathcal{M}_4, \quad E_6 \in \mathcal{M}_6, \quad E_4^2 \in \mathcal{M}_8, \quad E_4 \cdot E_6 \in \mathcal{M}_{10}, \quad E_4^2 \cdot E_6 \in \mathcal{M}_{14}$$

and that these functions generate $\mathcal{M}_k$, since $\dim_{\mathbb{C}} \mathcal{M}_k = 1$, by Lemma 3.6 (iv). Now let $k = 12$ or $k > 14$. Since k is even, we have

$$k = 4 \cdot m \quad \text{or} \quad k = 4 \cdot m + 2 = 4(m-1) + 6 \qquad (m \in \mathbb{N}, m \geq 3).$$

Therefore there exist $a, b \in \mathbb{N}$ such that $4a + 6b = k$. In this case it follows that

$$E_4^a \cdot E_6^b \in \mathcal{M}_k.$$

Let now $f \in \mathcal{M}_k$. Since $E_4(z)^a \cdot E_6(z)^b$ has no zero at ∞ (see its Fourier expansion), there exists a constant $c \in \mathbb{C}$ with

$$f - c \cdot E_4^a \cdot E_6^b \in \mathcal{S}_k.$$

By Proposition 3.7 (i), we thus get that

$$f - c \cdot E_4^a \cdot E_6^b = \Delta \cdot g$$

for some $g \in \mathcal{M}_{k-12}$. Therefore, we have

$$\begin{aligned} f(z) &= c \cdot E_4(z)^a \cdot E_6(z)^b + \Delta \cdot g \\ &= c \cdot E_4(z)^a \cdot E_6(z)^b + \left(\frac{E_4(z)^3 - E_6(z)^2}{1728}\right) \cdot g. \end{aligned}$$

Now the claim follows by a simple induction on k. ■

We end this chapter with some results for the j-function defined in (3.3).

Theorem 3.10 Let $f : \mathbb{H} \to \mathbb{C}$ be a meromorphic function. Then the following statements are equivalent:

(i) f is a modular function of weight 0 for Γ.

(ii) f is the quotient of two modular forms of the same weight for Γ.

(iii) f is a rational function in j, i.e. f is of the form

$$f(z) = \frac{F(j(z))}{G(j(z))}$$

for polynomials $F, G, G \neq 0$, with complex coefficients.

In particular, the field of all modular functions of weight 0 for Γ equals $\mathbb{C}(j)$.

Proof. Let $f : \mathbb{H} \to \mathbb{C}$ be a meromorphic function.

$(iii) \Longrightarrow (ii)$: Let $F = \sum_{r=0}^{n} a_r X^r$ and $G = \sum_{r=0}^{m} b_r X^r$ be two polynomials with complex coefficients with

$$f(z) = \frac{F(j(z))}{G(j(z))}.$$

Recalling that

$$j(z) = \frac{E_4(z)^3}{\Delta(z)},$$

we thus have

$$\begin{aligned} f(z) = \frac{F(j(z))}{G(j(z))} &= \frac{\sum_{r=0}^{n} a_r j(z)^r}{\sum_{r=0}^{m} b_r j(z)^r} = \frac{\sum_{r=0}^{n} a_r E_4(z)^{3r} \Delta(z)^{-r}}{\sum_{r=0}^{m} b_r E_4(z)^{3r} \Delta(z)^{-r}} \\ &= \frac{\Delta(z)^m \sum_{r=0}^{n} a_r E_4(z)^{3r} \Delta(z)^{n-r}}{\Delta(z)^n \sum_{r=0}^{m} b_r E_4(z)^{3r} \Delta(z)^{m-r}}, \end{aligned}$$

where we expanded the fraction in the last step by $\Delta(z)^n\Delta(z)^m$. This is a quotient of modular forms of the same weight $12(n+m)$. (Every term in the numerator has weight $12 \cdot m + 4 \cdot 3 \cdot r + 12 \cdot (n-r) = 12 \cdot (n+m)$ and a similar formula holds for the denominator.) This proves (ii).

$(ii) \Longrightarrow (i)$: Clear, by the definition of a modular function of weight 0 for Γ.

$(i) \Longrightarrow (iii)$: Let f be a modular function of weight 0 for Γ. Further, let $z_1, \ldots, z_r \in \mathcal{F}_\Gamma \cap \mathbb{H}$ be all the different poles of f in $\mathcal{F}_\Gamma \cap \mathbb{H}$, i.e. representative of the poles of f modulo Γ, and let $\nu_1, \ldots, \nu_r$ be the orders of these poles. Consider the function

$$h(z) := \prod_{k=1}^{r} \big(j(z) - j(z_k)\big)^{\nu_k}.$$

Then, the function

$$f(z)h(z)$$

is holomorphic on $\mathbb{H}$ by construction (since the function $h(z)$ has zeros of order at least ν_k in z_k). Hence, there exists $m \in \mathbb{N}$, such that the function

$$g(z) := f(z)h(z)(\Delta(z))^m$$

is holomorphic on $\mathbb{H}$ and at ∞. Therefore

$$g(z) \in \mathcal{M}_{12m}(\Gamma)$$

and, by Theorem 3.9, we can write $g(z)$ as a sum of terms of the form

$$E_4(z)^a\, E_6(z)^b \quad (a, b \in \mathbb{N}; 4a + 6b = 12m).$$

Now, since $h(z)$ is obviously the claimed form, it suffices to prove that the terms of the form

$$\frac{E_4(z)^a\, E_6(z)^b}{\Delta(z)^m}$$

can be written as rational functions in j. We note that, since $4a + 6b = 12m$, there exist natural numbers a', b' with

$$a = 3a',\ b = 2b' \ \text{ and } \ m = a' + b'.$$

Recalling that

$$\Delta(z) = \frac{E_4(z)^3 - E_6(z)^2}{1728} \Longleftrightarrow E_6(z)^2 = E_4(z)^3 - 1728\Delta(z),$$

we thus get

$$\begin{aligned} \frac{E_4(z)^a\, E_6(z)^b}{\Delta(z)^m} &= \frac{(E_4(z)^3)^{a'}}{\Delta(z)^{a'}} \frac{(E_6(z)^2)^{b'}}{\Delta(z)^{b'}} \\ &= j(z)^{a'} \frac{(E_4(z)^3 - 1728\Delta(z))^{b'}}{\Delta(z)^{b'}} \\ &= j(z)^{a'} \big(j(z) - 1728\big)^{b'}. \end{aligned}$$

This finishes the proof.

■

4. Modular forms of higher level

In this chapter we let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a subgroup of finite index.

4.1 Modular forms of weight k

Remark. We recall/refine some facts on cusps

(i) $\Gamma \setminus \mathbb{P}^1(\mathbb{Q})$ is the set of cusps of $\Gamma\backslash\mathbb{H}$ and $\#\Gamma \setminus \mathbb{P}^1(\mathbb{Q}) \leq [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$. Identifying $\mathbb{P}^1(\mathbb{Q})$ with $\mathbb{Q} \cup \{\infty\}$, we write a cusp $[a : c]$ often as $\frac{a}{c}$.

(b) $\mathrm{SL}_2(\mathbb{Z})_\infty = \left\{ \pm \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \mid m \in \mathbb{Z} \right\} = < \pm \mathrm{id}\,, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} >$

(c) Let $\sigma := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then the stabilizer of the cusp $\frac{a}{c}$ is given by

$$\Gamma_{\frac{a}{c}} = \Gamma \cap \sigma < \pm \mathrm{id}\,, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} > \sigma^{-1} = < \pm \mathrm{id}\,, \sigma \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \sigma^{-1} > .$$

Also, the width of the cusp $\frac{a}{c}$ is the smallest positive number h, such that

$$\sigma \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \sigma^{-1} \in \Gamma_{\frac{a}{c}} \qquad \text{or} \qquad \sigma \begin{pmatrix} -1 & -h \\ 0 & -1 \end{pmatrix} \sigma^{-1} \in \Gamma_{\frac{a}{c}}.$$

Then $\Gamma_{\frac{a}{c}}$ equals either $< \sigma \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \sigma^{-1} >, < -\mathrm{id}\,, \sigma \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \sigma^{-1} >$ or $< \sigma \begin{pmatrix} -1 & -h \\ 0 & -1 \end{pmatrix} \sigma^{-1} >$.

In the first two cases we say that $\frac{a}{c}$ is *regular*, in the last case we call $\frac{a}{c}$ *irregular*.

Remark. Irregular cusps are somehow exceptional, e.g. for $\Gamma_0(N)$ there are no irregular cusps (left as exercise).

Definition 4.1. Let $k \in \mathbb{Z}$, $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R})$ and $f : \mathbb{H} \longrightarrow \mathbb{C}$ be a function. We define $j(\gamma, z) := cz + d$ and

$$f|_k\gamma : \mathbb{H} \longrightarrow \mathbb{C}, \quad z \mapsto \det(\gamma)^{\frac{k}{2}} j(\gamma, z)^{-k} f(\gamma z).$$

The operator $f \mapsto f|_k\gamma$ is called *weight-k-operator*.

Remark. (a) If $f : \mathbb{H} \longrightarrow \mathbb{C}$ is holomorphic, then $f|_k\gamma$ is holomorphic for every $\gamma \in \Gamma$.
(b) Let $\gamma, \gamma' \in \mathrm{GL}_2^+(\mathbb{R})$, then $f|_k(\gamma\gamma') = (f|_k\gamma)|_k\gamma'$.

Definition 4.2. A *weak modular form of weight k for* Γ is a holomorphic function $f : \mathbb{H} \longrightarrow \mathbb{C}$ such that for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $z \in \mathbb{H}$ the transformation property

$$f(\gamma z) = (cz + d)^k f(z)$$

is satisfied, i.e. we have $f|_k\gamma = f$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$.

Proposition 4.3. Let $f : \mathbb{H} \longrightarrow \mathbb{C}$ be a weak modular form of weight k for Γ. Let $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and let $\tilde{h}$ be the width of the cusp $\frac{a}{c}$.
We set

$$h := \begin{cases} \tilde{h} & \text{if } \frac{a}{c} \text{ is regular} \\ 2\tilde{h} & \text{if } \frac{a}{c} \text{ is irregular} \end{cases}$$

Then the function $f|_k\sigma$ has a Fourier expansion of the form :

$$(f|_k\sigma)(z) = \sum_{n=-\infty}^{\infty} a_n e^{\frac{2\pi i n z}{h}} = \sum_{n=-\infty}^{\infty} a_n q^{\frac{n}{h}}.$$

Proof. It suffices to show that $f|_k\sigma$ has period h. Using the above remark, we compute

$$\begin{aligned} f|_k\sigma(z+h) &= (f|_k\sigma)|_k \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} (z) \\ &= f|_k \left(\sigma \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \sigma^{-1}\sigma \right) (z) \\ &= f|_k\sigma(z), \end{aligned}$$

which proves the claim. ■

Definition 4.4. Let f, σ, h and $\frac{a}{c}$ be as in the last Proposition. We call f *meromorphic at the cusp* $\frac{a}{c}$, if there exists $m \in \mathbb{Z}$ such that

$$f|_k\sigma(z) = \sum_{n=m}^{\infty} a_n q^{\frac{n}{h}}.$$

We say that f is *holomorphic at the cusp* $\frac{a}{c}$, if in addition $m \geq 0$, and we say that f *vanishes at the cusp* $\frac{a}{c}$, if $m \geq 1$.

Definition 4.5. A weak modular form f of weight k for Γ is called

- *modular function of weight k for* Γ, if f is meromorphic at all the cusps of Γ.
- *modular form of weight k for* Γ, if f is holomorphic at all the cusps of Γ.
- *cusp form of weight k for* Γ, if f vanishes at all cusps of Γ.

We use the notation

$$\mathcal{M}_k(\Gamma) := \{f \mid f \text{ is a modular form of weight } k \text{ for } \Gamma\},$$
$$\mathcal{S}_k(\Gamma) := \{f \mid f \text{ is a cusp form of weight } k \text{ for } \Gamma\}.$$

Remark. If f and g are two modular forms of weight k for Γ, then their sum $f+g$ is also a modular form of weight k for Γ, as is λf for any $\lambda \in \mathbb{C}$. Thus for any fixed weight k and congruence subgroup Γ we obtain a $\mathbb{C}$-vector space $\mathcal{M}_k(\Gamma)$ that contains the cusp forms $\mathcal{S}_k(\Gamma)$ as a subspace. The dimension of these vector spaces is finite, and can be explicitly in terms of invariants of the corresponding modular curve $\Gamma\backslash\mathbb{H}$.

Remark. Note that it suffices to check the 'cusp conditions' on a system of representatives of the cusps of Γ.

Using the Riemann–Roch theorem, one can prove the following dimension formulas.

Proposition 4.6. Let Γ be a congruence subgroup of genus g. For $k=0$, we have $\dim(\mathcal{M}_k(\Gamma)) = 1$ and $\dim(\mathcal{S}_k(\Gamma)) = 0$. For any even integer $k>0$, we have

$$\dim(\mathcal{M}_k(\Gamma)) = (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \nu_2 + \left\lfloor \frac{k}{3} \right\rfloor \nu_3 + \frac{k}{2}\nu_\infty.$$

For $k=2$, we have

$$\dim(\mathcal{S}_k(\Gamma)) = g$$

and for $k>2$, we have

$$\dim(\mathcal{S}_k(\Gamma)) = (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \nu_2 + \left\lfloor \frac{k}{3} \right\rfloor \nu_3 + \left(\frac{k}{2}-1\right)\nu_\infty.$$

Proof. See, e.g., Diamond and Shurman, Thm. 3.5.1. ∎

Remark. Use the commands *dimension_cusp_forms* and *dimension_modular_forms* to compute in *sagemath* the dimensions of, e.g., $\mathcal{S}_k(\Gamma_0(N))$ and $\mathcal{M}_k(\Gamma_0(N))$, respectively:

```
sage: dimension_cusp_forms(Gamma0(2007),2)
221
sage: dimension_modular_forms(Gamma0(2007),2)
228
```

Proposition 4.7. Let Γ be such that $\Gamma(N) \subseteq \Gamma$ for some $N \in \mathbb{N}$ and let f be a weak modular form of weight k for Γ, which is holomorphic at ∞. If there exists a constant $C>0$ such that

$$a_n \leq Cn^r$$

for all $n \in \mathbb{N}$, then f is a modular form of weight k for Γ.

Proof. At ∞ we have $f(z) = \sum_{n=0}^{\infty} a_n q^{\frac{n}{N}}$, since the width of every cusp divides N. First we are going to prove that there exists constants $C_0, C_1 > 0$ such that

$$|f(z)| \leq C_0 + C_1 \frac{1}{\mathrm{Im}(z)^r}.$$

To see this let $z = x + iy \in \mathbb{H}$. Then we have

$$\begin{aligned}
|f(z)| &= |\sum_{n=0}^{\infty} a_n q^{\frac{n}{N}}| \\
&\leq \sum_{n=0}^{\infty} |a_n| e^{-\frac{2\pi n y}{N}} \\
&\leq |a_0| + C\sum_{n=1}^{\infty} n^r e^{-\frac{2\pi n y}{N}} \\
&= |a_0| + C\left(\frac{N}{2\pi}\right)^r \frac{1}{y^r} \sum_{n=1}^{\infty} \left(\frac{2\pi y n}{N}\right)^r e^{-\frac{2\pi n y}{N}} \\
&< |a_0| + C\left(\frac{N}{2\pi}\right)^r \frac{1}{y^r} C_2 \Gamma(r+1) \\
&=: C_0 + C_1 \frac{1}{y^r}.
\end{aligned}$$

We now prove that f is holomorphic at the cusps. For $\sigma \mathrm{SL}_2(\mathbb{Z})$ let $f|_k\sigma(z) = \sum_{n=-\infty}^{\infty} b_n q^{\frac{n}{N}}$. It suffices to show that

$$\lim_{\mathrm{Im}(z)\to\infty} q^{\frac{1}{N}} (f|_k\sigma)(z) = 0.$$

We use that $|cz+d|$ behaves as $|c|\mathrm{Im}(z)$ for large $\mathrm{Im}(z)$ and $\mathrm{Re}(z) \leq N$. We compute

$$\begin{aligned}
|f|_k\sigma(z)| &= \frac{1}{|cz+d|^k} \left| f\left(\frac{az+b}{cz+d}\right)\right| \\
&\leq \frac{1}{|cz+d|^k} \left| C_0 + C_1 \mathrm{Im}\left(\frac{az+b}{cz+d}\right)^{-r}\right| \\
&= \frac{1}{|cz+d|^k} \left| C_0 + C_1 \frac{|cz+d|^{2r}}{\mathrm{Im}(z)^r}\right| \\
&\underset{\text{for large } \mathrm{Im}(z)}{<} C_3 \mathrm{Im}(z)^{r-k}.
\end{aligned}$$

for some constant $C_3 > 0$.
Hence

$$\lim_{\mathrm{Im}(z)\to\infty} |q^{\frac{1}{N}} (f|_k\sigma)(z)| \leq \lim_{\mathrm{Im}(z)\to\infty} |e^{-2\pi \mathrm{Im}(z)} C_3 \mathrm{Im}(z)^{r-k}| = 0.$$

This proves the claim. ■

Remark. Let $\Gamma \subseteq \Gamma' \subseteq \mathrm{SL}_2(\mathbb{Z})$ be subgroups of finite index. Then every modular form of weight k for Γ' is a modular form of weight k for Γ. The same statement holds for modular functions and cusp forms.

Definition 4.8. Let f be a modular form of weight k for $\Gamma_1(N)$ and let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ be a Dirichlet character. We say that f has character χ if

$$f(\gamma z) = \chi(d)(cz+d)^k f(z)$$

for all $\gamma \in \Gamma_0(N)$.

Remark. If χ is trivial, i.e. $\chi(n) = 1$ for all $n : (n, N) = 1$, then a modular form for $\Gamma_1(N)$ has character χ, if it is a modular form for $\Gamma_0(N)$.

Notation 4.1.

$$\mathcal{M}_k(\Gamma,\chi) := \{f \mid f \textit{ is a mod. form of weight } k \textit{ for } \Gamma \textit{ and has character } \chi\}$$
$$\mathcal{S}_k(\Gamma,\chi) := \{f \mid f \textit{ is a cusp form of weight } k \textit{ for } \Gamma \textit{ and has character } \chi\}$$

4.2 Old and new forms

We first define old forms. The newforms then are defined in the next chapter as a vector subspace of the modular forms of level N, complementary to the space spanned by the oldforms, i.e. the orthogonal space with respect to the Petersson inner product.

Proposition 4.9. Let $M, N \in \mathbb{N}$ and let f be a modular form of weight k with respect to $\Gamma_0(N)$. Then for any divisor $m \mid M$, the function

$$g(z) := f(mz)$$

is a modular form of weight k for $\Gamma_0(NM)$. The analogous statement holds for cusp forms.

Proof. Clearly g is holomorphic on $\mathbb{H}$, since f is holomorphic on $\mathbb{H}$.
Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(NM)$. We observe that $\begin{pmatrix} a & bm \\ \frac{c}{m} & d \end{pmatrix} \in \Gamma_0(N)$. Hence

$$\begin{aligned} g\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z\right) &= f\left(m\frac{az+b}{cz+d}\right) \\ &= f\left(\frac{a(mz)+bm}{\frac{c}{m}(mz)+d}\right) \\ &= (\frac{c}{m}(mz)+d)^k f(mz) \\ &= (cz+d)^k g(z). \end{aligned}$$

To see the holomorphicity at the cusps let $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and let $\rho := (c, ma)$. We can find $r, s \in \mathbb{Z} : \rho = sc + rma$ (eucl. algorithm). Then

$$\alpha := \begin{pmatrix} -r & -s \\ \frac{c}{\rho} & -\frac{ma}{\rho} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

and

$$\alpha \begin{pmatrix} ma & mb \\ c & d \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & v \end{pmatrix}$$

with $x, y, v \in \mathbb{Z}$.
Hence

$$\begin{pmatrix} ma & mb \\ c & d \end{pmatrix} = \alpha^{-1} \begin{pmatrix} x & y \\ 0 & v \end{pmatrix} := (*)$$

Since $g = f|_k \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$ we get

$$\begin{aligned} g|_k\sigma(z) &= f|_k \begin{pmatrix} ma & mb \\ c & d \end{pmatrix}(z) \\ &= f|_k \left(\alpha^{-1}\begin{pmatrix} x & y \\ 0 & v \end{pmatrix}\right)(z) \\ &= \frac{1}{z^k}(f|_k\alpha^{-1})\left(\frac{xz+y}{v}\right). \end{aligned}$$

Since f is a modular form, the limit $\lim\limits_{\mathrm{Im}(z)\to\infty} f|_k\alpha^{-1}(z)$ exists. Let this limit be denoted by C. Then

$$\lim_{\mathrm{Im}(z)\to\infty}\frac{1}{z^k}(f|_k\alpha^{-1})\left(\frac{xz+y}{v}\right) = \frac{C}{z^k} < \infty.$$

This proves the holomorphicity at the cusp $\frac{a}{c}$. If f is a cusp form, then $C = 0$ and therefore g is also a cusp form. ■

Definition 4.10. A modular form of weight k for $\Gamma_0(N)$ is called *old form*, if it is a linear combination of modular forms

$$g_i(d_i z),$$

where $M_i > 1$ is a divisor of N, $d_i \geq 1$ is a divisor of M_i and the g_i are modular forms of weight k for $\Gamma_0\left(\frac{N}{M_i}\right)$.

5. Theory of Hecke Operators

In order to understand the relationship between modular forms and elliptic curves we need to construct a suitable basis for $S_2(\Gamma_0(N))$. To do this, we use the theory of Hecke operators. For any $n \in \mathbb{N}_{\geq 1}$ the Hecke operator $T(n)$ (sometimes also denoted by T_n) is a linear operator that can be applied to any of the vector spaces $M_k(\Gamma_0(N))$, and it fixes the subspace of cusp forms, so it is also a linear operator on $S_k(\Gamma_0(N))$.

5.1 Theory of Hecke Operators for $\mathrm{SL}_2(\mathbb{Z})$

In this section we let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and $k \geq 1$ be an even(!) natural number. Note that it is possible to generalize the following results for arbitrary congruence subgroups. So the case $M_k(\Gamma_0(N))$ is analogous, but the details are more involved and we address $N > 1$ shortly in the next section.

We start by defining *the n-th Hecke-Operator* $T(n)$ for $(n \in \mathbb{N}_{\geq 1})$ on the space $\mathcal{M}_k(\Gamma)$.

Definition 5.1. Let $\bigcup_j \Gamma\gamma_j$ be a decomposition of the double coset $\Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma$ in (finitely many) left cosets $\Gamma\gamma_j$. Then, for $f \in \mathcal{M}_k(\Gamma)$, we set

$$f|T(n)(z) := f|_k\Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma(z) := n^{\frac{k}{2}-1} \sum_j f|_k\gamma_j.$$

Remark. One can easily see that the definition of the Hecke Operator is independent of the choice of the system of representatives $\{\gamma_j\}$.

Lemma 5.2. For $n \in \mathbb{N}_{\geq}$ we have the disjoint union

$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma = \bigcup_{\substack{a>0 \\ ad=n \\ b \mod d}} \Gamma \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Proof. We have to show that, for every $\gamma \in \Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma$, there exists a unique $A \in \Gamma$ (and unique $a > 0, ad = n,\ b \mod d$) such that

$$A\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Existence: Let

$$\gamma := \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma$$

with $c' \neq 0$. We write $-\frac{a'}{c'}$ in reduced form, i.e.

$$-\frac{a'}{c'} = \frac{r}{s} \qquad \Longleftrightarrow \qquad a's + c'r = 0,$$

where $r, s \in \mathbb{Z}$ with $(r, s) = 1$. By the euclidean algorithm, we can find $p, q \in \mathbb{Z}$ such that

$$rp - sq = 1.$$

Now, multiplication from the left by $A' := \begin{pmatrix} p & q \\ s & r \end{pmatrix} \in \Gamma$ yields

$$A'\gamma = \begin{pmatrix} p & q \\ s & r \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a & b'' \\ 0 & d \end{pmatrix},$$

where without loss of generality we can assume $a > 0$. Since $\gamma \in \Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma$, we have $\det(\gamma) = n$, and therefore

$$a > 0 \qquad \text{and} \qquad ad = n.$$

Finally, multiplication from the left by an appropriate matrix $A'' = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, the condition

$$b \mod d$$

can be satisfied as well. This also shows that the existence in case $c' = 0$ is trivial.
Uniqueness: Let $\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$ with $a_j > 0$, $a_j d_j = n$ and $b_j \mod d_j$ $(j = 1, 2)$ be two "representatives” of γ. Then there exists $B = \begin{pmatrix} \alpha & \beta \\ \eta & \delta \end{pmatrix} \in \Gamma$ with

$$\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \eta & \delta \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}.$$

Comparing coefficients yields $\eta = 0$ (since $a_1 > 0$). Without loss of generality we can therefore assume $\alpha = \delta = 1$, i.e. we have

$$\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}.$$

This yields
$$a_2 = a_1,\, d_2 = d_1,$$
and
$$b_2 = b_1 + \beta d_1 \equiv b_1 \mod d_1.$$
This proves that the "representation" $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with $a > 0$, $ad = n$ and $b \mod d$ is unique.

■

Remark. For $f \in \mathcal{M}_k(\Gamma)$ and $n \in \mathbb{N}_{\geq 1}$, we get
$$\begin{aligned} f|T(n)(z) &= n^{k-1} \sum_{\substack{a>0 \\ ad=n \\ b \mod d}} d^{-k} f\left(\frac{az+b}{d}\right) \\ &= n^{-1} \sum_{\substack{a>0 \\ ad=n \\ b \mod d}} a^k f\left(\frac{az+b}{d}\right). \end{aligned}$$

Proposition 5.3. For $n \in \mathbb{N}_{\geq 1}$, we have
$$f \in \mathcal{M}_k(\Gamma) \Longrightarrow f|T(n) \in \mathcal{M}_k(\Gamma).$$

Proof. The last remark yields the proof of holomorphicity of $f|T(n)$ on $\mathbb{H}$, since f is holomorphic on $\mathbb{H}$. It remains to show that $f|T(n)$ has weight k with respect to Γ and that the Fourier expansion of $f|T(n)$ in ∞ starts with an index ≥ 0, and that $f|T(n)$ has weight k w.r.t. to Γ.
To prove the last assertion, we work from the decomposition given in Lemma 5.2, namely, for $n \in \mathbb{N}_{\geq}$, we have
$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma = \bigcup_{\substack{a>0 \\ ad=n \\ b \mod d}} \Gamma \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$
We need the following Lemma:

Lemma 5.4. Assume the above notation and let $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \Gamma$. Then there exist $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, $M' = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$ in the above decomposition such that
$$MA = A'M',\;\; A' := \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} \in \Gamma$$
and $a'(\gamma z + \delta) = a(\gamma' M' z + \delta')$.

Proof. Since $MA \in \Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma$, the existence of A', M' follows from Lemma 5.2. To prove the second claim we observe
$$\begin{aligned} \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} = A' = MAM'^{-1} &= \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \frac{1}{n} \begin{pmatrix} d' & -b' \\ 0 & a' \end{pmatrix} \\ &= \frac{1}{n} \begin{pmatrix} * & * \\ d\gamma & d\delta \end{pmatrix} \begin{pmatrix} d' & -b' \\ 0 & a' \end{pmatrix} = \frac{1}{n} \begin{pmatrix} * & * \\ dd'\gamma & -db'\gamma + da'\delta \end{pmatrix}. \end{aligned}$$

Comparing coefficients yields (recalling that $ad = n$, $a > 0$)

$$\gamma' = \frac{dd'\gamma}{n} = \frac{d'}{a}\gamma$$
$$\delta' = \frac{-db'\gamma + da'\delta}{n} = -\frac{b'}{a}\gamma + \frac{a'}{a}\delta.$$

In other words, we get (observe for (i) that $d' \neq 0$)

$$(i) \qquad a\gamma' = d'\gamma \Rightarrow \frac{a\gamma'}{d'} = \gamma$$

and

$$(ii) \qquad a\delta' = -b'\gamma + a'\delta.$$

This results in (in the third step we employ (i) and (ii))

$$\begin{aligned} a(\gamma' M' z + \delta') &= a\left(\gamma' \frac{a'z + b'}{d'} + \delta'\right) \\ &= \frac{a\gamma' a' z}{d'} + \frac{a\gamma' b'}{d'} + a\delta' \\ &= a'\gamma z + b'\gamma - b'\gamma + a'\delta \\ &= a'(\gamma z + \delta), \end{aligned}$$

as asserted. ■

With the help of Lemma 5.4, we are now going to prove that $f|T(n)$ has weight k with respect to Γ. Let $f \in \mathcal{M}_k(\Gamma)$ and $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \Gamma$. We have (using $\det(A) = 1$)

$$\begin{aligned} (f|T(n))|_k A(z) &= n^{-1} \sum_{\substack{a>0, ad=n \\ b \mod d}} a^k f(MAz)(\gamma z + \delta)^{-k} \\ &\overset{\text{Lemma 5.4}}{=} n^{-1} \sum_{\substack{a'>0, a'd'=n \\ b' \mod d}} a'^k f(A'M'z)(\gamma' M' z + \delta')^{-k} \\ &= n^{-1} \sum_{\substack{a'>0, a'd'=n \\ b' \mod d}} a'^k f|_k A'(M'z) \\ &\overset{\substack{A' \in \Gamma \\ f \in \mathcal{M}_k(\Gamma)}}{=} n^{-1} \sum_{\substack{a'>0, a'd'=n \\ b' \mod d}} a'^k f(M'z). \end{aligned}$$

If M runs through a complete system of representatives of cosets $\Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma$, then M' will do so as well. Hence

$$(f|T(n))|_k A = f|T(n),$$

and, since $A \in \Gamma$ was arbitrary, this yields the assertion.
Finally, we are going to show that $f|T(n)$ is holomorphic at ∞ by studying its Fourier expansion. Let $f \in \mathcal{M}_k(\Gamma)$ and let

$$f(z) = \sum_{m=0}^{\infty} a(m)\, e^{2\pi i m z}$$

be its Fourier expansion. Then, $f|T(n)$ has the expansion

$$
\begin{aligned}
f|T(n)(z) &= n^{k-1} \sum_{\substack{a>0, ad=n \\ b \mod d}} d^{-k} f\left(\frac{az+b}{d}\right) \\
&= n^{k-1} \sum_{d\,|\,n} d^{-k} \sum_{b=0}^{d-1} \sum_{m=0}^{\infty} a(m)\, e^{2\pi i m\left(\frac{nz+bd}{d^2}\right)} \\
&= \sum_{m=0}^{\infty} \sum_{d\,|\,n} \left(\frac{n}{d}\right)^{k-1} a(m)\, e^{2\pi i m n z/d^2} \frac{1}{d} \sum_{b=0}^{d-1} e^{2\pi i m b/d} \\
&= \sum_{m=0}^{\infty} \sum_{\substack{d\,|\,m \\ d\,|\,n}} \left(\frac{n}{d}\right)^{k-1} a(m)\, e^{2\pi i m n z/d^2} \\
&\overset{m=m'd}{=} \sum_{m'=0}^{\infty} \sum_{d\,|\,n} \left(\frac{n}{d}\right)^{k-1} a(m'd)\, e^{2\pi i m' n z/d} \\
&\overset{d'=n/d}{=} \sum_{m'=0}^{\infty} \sum_{d'\,|\,n} d'^{k-1} a(\frac{m'n}{d'})\, e^{2\pi i m' d' z} \\
&\overset{m=m'd'}{=} \sum_{m=0}^{\infty} \sum_{\substack{d'\,|\,m \\ d'\,|\,n}} d'^{k-1} a(\frac{mn}{d'^2})\, e^{2\pi i m z}.
\end{aligned}
$$

Here, for the 4th identity, we observe that

$$
\frac{1}{d} \sum_{b=0}^{d-1} e^{2\pi i m b/d} = \begin{cases} 1, & \text{if } d|m; \\ 0, & \text{else}. \end{cases}
$$

Hence, $f|T(n)$ has the Fourier expansion

$$
f|T(n)(z) = \sum_{m=0}^{\infty} a'(m) q^m \tag{5.1}
$$

with

$$
a'(m) := \sum_{d\,|\,(m,n)} d^{k-1} a\left(\frac{mn}{d^2}\right). \tag{5.2}
$$

Therefore, all in all, we have shown that $f|T(n) \in \mathcal{M}_k(\Gamma)$. This completes the proof. ■

Remark. The above proof also shows:

(i) Let $f \in \mathcal{M}_k(\Gamma)$ and let

$$
f(z) = \sum_{m=0}^{\infty} a(m)\, e^{2\pi i m z}
$$

be its Fourier expansion. Then, the Fourier expansion of $f|T(n)$ is of the form (5.1) with coefficients given by (5.2). In particular, we have

$$
a'(0) = \sigma_{k-1}(n) a(0) \qquad \text{and} \qquad a'(1) = a(n).
$$

(ii) $f \in \mathcal{S}_k(\Gamma) \Rightarrow f|T(n) \in \mathcal{S}_k(\Gamma)$.

Corollary 5.5. For $n = p$, p prime, the m-th Fourier coefficient $a'(m)$ of $f \mid T(p)$ ($m \in \mathbb{N}$) satisfies the identity

$$a'(m) = a(mp) + p^{k-1} a\left(\frac{m}{p}\right),$$

where we have set $a(\frac{m}{p}) := 0$, if $\frac{m}{p} \notin \mathbb{Z}$.

Proposition 5.6. For all $m, n \in \mathbb{N}_{\geq 1}$ with $(m, n) = 1$, we have

$$T(mn) = T(m)T(n).$$

Proof. We consider the action of $T(mn)$ and $T(m)T(n)$ on elements $f \in \mathcal{M}_k(\Gamma)$. We have

$$\begin{aligned}
((f|T(m))|T(n))(z) &= \left(\frac{1}{m} \sum_{\substack{\alpha>0, \alpha\delta=m \\ \beta \mod \delta}} \alpha^k f\left(\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} z\right)\right) \Bigg| T(n) \\
&= \frac{1}{m} \sum_{\substack{\alpha>0, \alpha\delta=m \\ \beta \mod \delta}} \alpha^k \frac{1}{n} \sum_{\substack{a>0, ad=n \\ b \mod d}} a^k f\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} z\right) \\
&= \frac{1}{mn} \sum_{\substack{\alpha>0, \alpha\delta=m \\ \beta \mod \delta}} \sum_{\substack{a>0, ad=n \\ b \mod d}} (a\alpha)^k f\left(\begin{pmatrix} a\alpha & a\beta + b\delta \\ 0 & d\delta \end{pmatrix} z\right).
\end{aligned}$$

If a (respectively α) runs through all positive divisors of n (resp. m), then $a' := a\alpha$ runs through all positive divisors of mn (since $(m, n) = 1$). By the chinese remainder theorem we also know that if b (resp. β) runs through all remainders $\mod d$ (resp. $\mod \delta$) then $b' := a\beta + b\delta$ runs through all remainders $\mod d' := d\delta$. Hence, we get

$$\begin{aligned}
((f|T(m))|T(n))(z) &= \frac{1}{mn} \sum_{\substack{a'>0, a'd'=mn \\ b' \mod d'}} (a')^k f\left(\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} z\right) \\
&= f|T(mn)(z).
\end{aligned}$$

This proves the claim. ■

Proposition 5.7. Let $r \in \mathbb{N}_{\geq 1}$ and let p be a prime number. Then, we have

$$T(p^r)T(p) = T(p^{r+1}) + p^{k-1}T(p^{r-1}).$$

Proof. First we observe that, for $f, g \in \mathcal{M}_k(\Gamma)$, we have

(i)

$$f|T(p^r)(z) = p^{-r} \sum_{\substack{0 \leq t \leq r \\ 0 \leq b_t < p^t}} p^{(r-t)k} f\left(\frac{p^{r-t}z + b_t}{p^t}\right)$$

(ii)

$$g|T(p)(z) = p^{k-1}g(pz) + p^{-1} \sum_{0 \leq b < p} g\left(\frac{z+b}{p}\right).$$

Thus, for $f \in \mathcal{M}_k(\Gamma)$, we get

$$\begin{aligned}
((f|T(p^r))|T(p))(z) &= p^{-r} \sum_{\substack{0\le t\le r\\ 0\le b_t<p^t}} p^{(r-t)k} \left(p^{k-1} f\left(p\frac{p^{r-t}z+b_t}{p^t}\right) + p^{-1}\sum_{0\le b<p} f\left(\frac{\frac{p^{r-t}z+b_t}{p^t}+b}{p}\right)\right) \\
&= p^{k-1-r} \sum_{\substack{0\le t\le r\\ 0\le b_t<p^t}} p^{(r-t)k} f\left(\frac{p^{r+1-t}z+pb_t}{p^t}\right) + \\
&\quad p^{-1-r} \sum_{\substack{0\le t\le r\\ 0\le b_t<p^t}} p^{(r-t)k} \sum_{0\le b<p} f\left(\frac{p^{r-t}z+p^tb+b_t}{p^{t+1}}\right) \\
&= p^{-1-r} \sum_{\substack{0\le t\le r\\ 0\le b_t<p^t}} p^{(r+1-t)k} f\left(\frac{p^{r-t}z+b_t}{p^{t-1}}\right) + \\
&\quad p^{-1-r} \sum_{\substack{0\le t\le r\\ 0\le b_t<p^t}} \sum_{0\le b<p} p^{((r+1)-(t+1))k} f\left(\frac{p^{(r+1)-(t+1)}z+p^tb+b_t}{p^{t+1}}\right) \\
&= p^{-1-r} \sum_{\substack{0<t\le r\\ 0\le b_t<p^t}} p^{(r+1-t)k} f\left(\frac{p^{r-t}z+b_t}{p^{t-1}}\right) + \\
&\quad p^{-1-r} \sum_{\substack{0\le t'\le r+1\\ 0\le b'_{t'}<p^{t'}}} p^{((r+1)-t')k} f\left(\frac{p^{r+1-t'}z+b'_{t'}}{p^{t'}}\right) \\
&= p^{-1-r} \sum_{\substack{1\le t\le r\\ 0\le b_t<p^t}} p^{(r+1-t)k} f\left(\frac{p^{r-t}z+b_t}{p^{t-1}}\right) + f|T(p^{r+1})(z).
\end{aligned}$$

Let us now write b_t in the form

$$b_t = q_t p^{t-1} + r_t\ ,\ 0 \le r_t < p^{t-1}.$$

Then, b_t runs through a complete system of representatives mod p^t, if r_t runs through a complete system of representatives mod p^{t-1} and q_t runs through a complete system of representatives mod p. Hence

$$f\left(\frac{p^{r-t}z+b_t}{p^{t-1}}\right) = f\left(\frac{p^{r-t}z+r_t}{p^{t-1}}+q_t\right) = f\left(\frac{p^{r-t}z+r_t}{p^{t-1}}\right)$$

and also

$$\begin{aligned}
((f|T(p^r))|T(p))(z) &= f|T(p^{r+1})(z) + p\,p^{-1-r} \sum_{\substack{1\le t\le r\\ 0\le r_t<p^{t-1}}} p^{(r-(t-1))k} f\left(\frac{p^{(r-1)-(t-1)}z+r_t}{p^{t-1}}\right) \\
&= f|T(p^{r+1})(z) + p^{k-1}\,p^{-(r-1)} \sum_{\substack{0\le t'\le r-1\\ 0\le r'_{t'}<p^{t'}}} p^{(r-1-t')k} f\left(\frac{p^{r-1-t'}z+r'_{t'}}{p^{t'}}\right) \\
&= f|T(p^{r+1})(z) + p^{k-1}\, f|T(p^{r-1})(z).
\end{aligned}$$

This finishes the proof. ■

Remark. The above propositions show that it suffices to understand the behavior of $T(p)$ for p prime.

Corollary 5.8. For $m, n \in \mathbb{N}_{\geq 1}$, we have

$$T(m)T(n) = \sum_{d \mid (m,n)} d^{k-1} T\left(\frac{mn}{d^2}\right).$$

In particular, we have

$$T(m)T(n) = T(n)T(m).$$

Proof. If $(m, n) = 1$ the first assertion follows from Proposition 5.6. It remains to prove the first claim for $m = p^r, n = p^s$, i.e., we have to show that

$$T(p^r)T(p^s) = \sum_{t=0}^{r} p^{t(k-1)} T(p^{r+s-2t})$$

for all r and $s \geq r$. This can be done by using Proposition 5.7 and induction (exercise). The second claim clearly follows from the first claim. ∎

Remark. Consider

$$\mathcal{H} := \left\{ \sum_{n=1}^{\infty} c_n T(n) \mid c_n \in \mathbb{C},\, c_n = 0 \text{ for almost all } n \right\}.$$

By Corollary 5.8, $\mathcal{H}$ is a commutative $\mathbb{C}$-algebra, called the *Hecke algebra*. We have also seen that $\mathcal{H}$ is a commutative subalgebra of $\mathrm{End}(\mathcal{M}_k(\Gamma))$, generated by all $T(p)$ for p a prime number.

We now define a scalar product $\langle \cdot, \cdot \rangle$ on $\mathcal{S}_k(\Gamma)$. We will see that the Hecke operators are self-adjoint with respect to $\langle \cdot, \cdot \rangle$.

Definition 5.9. Let $f, g \in \mathcal{M}_k(\Gamma)$, where at least one of them is a cusp form. Then, the *Petersson scalar product of f and g* is defined by

$$\langle f, g \rangle := \int_{\Gamma \backslash \mathbb{H}} f(z)\overline{g(z)} \mathrm{Im}(z)^k \mu_{\mathrm{hyp}}(z),$$

where $z = x + iy$ and $\mu_{\mathrm{hyp}}(z) = dxdy/y^2$.

Proposition 5.10. Let $f, g \in \mathcal{M}_k(\Gamma)$, where at least one of them is a cusp form. Then, $\langle f, g \rangle$ converges absolutely and satisfies the following properties:
(i) $\langle f, g \rangle$ is linear in f, and conjugate linear in g.
(ii) $\langle f, g \rangle = \overline{\langle g, f \rangle}$.
(iii) $\langle f, f \rangle \geq 0$ for $f \in \mathcal{S}_k(\Gamma)$, and $\langle f, f \rangle = 0 \iff f = 0$.
In particular, $\langle \cdot, \cdot \rangle$ defines a scalar product on $\mathcal{S}_k(\Gamma)$.

Proof. If $f \in \mathcal{S}_k(\Gamma)$ or $g \in \mathcal{S}_k(\Gamma)$, then

$$fg \in \mathcal{S}_{2k}(\Gamma),$$

and the function $|f(z)g(z)|y^k$ is bounded on $\mathbb{H}$. Since $\mathrm{vol}_{\mathrm{hyp}}(\Gamma\backslash\mathbb{H}) < \infty$, this yields the absolute convergence of $\langle f, g\rangle$. The properties (i), (ii), and (iii), now easily follow using the definition of $\langle\cdot,\cdot\rangle$. ∎

Remark. To explicitly compute the Petersson scalar product $\langle f, g\rangle$, we usually choose a fundamental domain $\mathcal{F}$ for $\Gamma\backslash\mathbb{H}$, and we note that the result doesn't depend on the choice of $\mathcal{F}$.

We now compute the Petersson scalar product of a cusp form and of the normalized Eisenstein series E_k of weight k.

Proposition 5.11. Let $k \geq 4$ be an even integer. For $f \in \mathcal{S}_k(\Gamma)$, we have

$$\langle E_k, f\rangle = 0.$$

Proof. We start by writing

$$E_k(z) = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} 1|_k\gamma,$$

with $\Gamma_\infty = \{\pm\left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right) \mid n \in \mathbb{Z}\}$. We then compute (using the absolute convergence)

$$\begin{aligned}\langle E_k, f\rangle &= \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \int_{\Gamma\backslash\mathbb{H}} j(\gamma,z)^{-k}\overline{f(z)}\mathrm{Im}(z)^k\mu_{\mathrm{hyp}}(z)\\ &= \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \int_{\Gamma\backslash\mathbb{H}} \overline{f(\gamma z)}\mathrm{Im}(\gamma z)^k\mu_{\mathrm{hyp}}(\gamma z),\end{aligned}$$

where for the second identity we used the Γ-invariance of $\mu_{\mathrm{hyp}}(z)$ and the identities

$$\begin{aligned}\mathrm{Im}(\gamma z)^k &= \mathrm{Im}(z)^k j(\gamma,z)^{-k}\overline{j(\gamma,z)}^{-k},\\ \overline{f(\gamma z)} &= \overline{f(z)}\cdot\overline{j(\gamma,z)}^k.\end{aligned}$$

We now consider the standard fundamental domain $\mathcal{F}$ of $\Gamma\backslash\mathbb{H}$. We first substitute $w := \gamma z$, and we obtain, applying the so-called unfolding method, the identity

$$\begin{aligned}\langle E_k, f\rangle &= \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \int_{\gamma\mathcal{F}} \overline{f(w)}\mathrm{Im}(w)^k\mu_{\mathrm{hyp}}(w)\\ &= \int_{\Gamma_\infty\backslash\mathbb{H}} \overline{f(z)}\mathrm{Im}(z)^k\mu_{\mathrm{hyp}}(z).\end{aligned}$$

With $z = x + iy$ and substituting the Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a(n)q^n$$

of f (with $a(0) = 0$, since f is a cusp form), we now compute (using the standard fundamental domain for $\Gamma_\infty\backslash\mathbb{H}$)

$$\langle E_k, f\rangle = \int_0^\infty\int_0^1 \overline{f(z)}dx\frac{dy}{y^{2-k}} = a(0)\int_0^\infty \frac{dy}{y^{2-k}} = 0,$$

as asserted. ∎

Remark. The above result shows that the decomposition

$$\mathcal{M}_k(\Gamma) = \mathbb{C}E_k \oplus \mathcal{S}_k(\Gamma)$$

is orthogonal with respect to the Petersson scalar product $\langle \cdot, \cdot \rangle$.

Before coming back to Hecke operators, we will find generators of $\mathcal{S}_k(\Gamma)$.

Definition 5.12. Let $k \geq 4$ be an even integer. For $m \in \mathbb{N}_{\geq 1}$, we define the *$m$-th Poincaré series (of weight k)* by

$$P_{m,k}(z) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} e^{2\pi i m z}|_k \gamma$$

Remark. Note that in case $m = 0$ this definition would lead to

$$P_{0,k}(z) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} 1|_k \gamma = E_k(z).$$

That's why we assume $m \in \mathbb{N}_{\geq 1}$.

Proposition 5.13. Let $k \geq 4$ be an even integer and let $m \in \mathbb{N}_{\geq 1}$. Then, we have

$$P_{m,k}(z) \in \mathcal{S}_k(\Gamma),$$

and, for any cusp form $f \in \mathcal{S}_k(\Gamma)$ with Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a(n) q^n,$$

we have

$$\langle f, P_{m,k} \rangle = \frac{(k-2)!}{(4\pi m)^{k-1}} a(m).$$

Further, the Poincaré series $P_{m,k}$ with $m \in \mathbb{N}_{\geq 1}$ span the vector space $\mathcal{S}_k(\Gamma)$.

Proof. The absolute and locally uniform convergence of $P_{m,k}$ can be proven analogously as for E_k. Hence, $P_{m,k}$ transforms like a modular form of weight k for Γ, by construction. Furthermore, we have

$$\lim_{y \to \infty} |P_{m,k}(z)| \leq \frac{1}{2} \sum_{\substack{(c,d) \in \mathbb{Z}^2 \\ (c,d)=1}} \lim_{y \to \infty} \exp\left(-2\pi m y / |cz+d|^2\right) |cz+d|^{-k} = 0.$$

Hence, we get

$$P_{m,k}(z) \in \mathcal{S}_k(\Gamma),$$

as claimed. Now, let $f \in \mathcal{S}_k(\Gamma)$ be a cusp form with Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a(n) q^n.$$

Using the unfolding method, we get

$$\langle f, P_{m,k}\rangle = \int_0^\infty \int_0^1 f(z) e^{-2\pi i m x} dx\, e^{-2\pi m y} \frac{dy}{y^{2-k}} = a(m) \int_0^\infty e^{-4\pi m y} \frac{dy}{y^{2-k}}$$
$$= a(m) \frac{\Gamma(k-1)}{(4\pi m)^{k-1}} = a(m) \frac{(k-2)!}{(4\pi m)^{k-1}},$$

as asserted.
Finally, let $\mathcal{P}$ be the subspace of $\mathcal{S}_k(\Gamma)$ spanned by the Poincaré series $P_{m,k}$ with $m \in \mathbb{N}_{\geq 1}$, and let $\mathcal{P}' \subseteq \mathcal{S}_k(\Gamma)$ denote its orthogonal complement. Let $f \in \mathcal{P}'$. Then, the Fourier coefficients $a(m)$ of f, satisfy identity

$$a(m) = \frac{(4\pi m)^{k-1}}{(k-2)!} \langle f, P_{m,k}\rangle = 0,$$

for all $m \in \mathbb{N}_{\geq 1}$, and trivially we have $a(0) = 0$. Hence $f = 0$. This proves $\mathcal{P} = \mathcal{S}_k(\Gamma)$, as claimed. ■

Now, we study so-called Hecke eigen forms.

Definition 5.14. A modular form $0 \neq f \in \mathcal{M}_k(\Gamma)$ is called *Hecke eigenform* (or *eigenform with respect to* $\mathcal{H}$), if f is an eigenfunction for all $T(n)$, i.e. for any $n \in \mathbb{N}_{\geq 1}$ there exists an eigenvalue $\lambda(n) \in \mathbb{C}$ such that

$$f|T(n) = \lambda(n) f.$$

Proposition 5.15. Let $0 \neq f \in \mathcal{M}_k(\Gamma)$ be a Hecke eigenform with Fourier expansion $f(z) = \sum_{m=0}^\infty a(m) e^{2\pi i m z}$, then

$$a(n) = \lambda(n) a(1)$$

for all $n \in \mathbb{N}_{\geq 1}$.

Proof. Let $0 \neq f \in \mathcal{M}_k(\Gamma)$ be a Hecke eigenform with Fourier expansion $f(z) = \sum_{m=0}^\infty a(m) e^{2\pi i m z}$. On the one hand (see Remark 5.1), we then have

$$f|T(n) = \sum_{m=0}^\infty a'(m) e^{2\pi i m z},$$

where

$$a'(1) = a(n).$$

On the other hand, we have

$$f|T(n) = \lambda(n) f = \sum_{m=0}^\infty \lambda(n) a(m) e^{2\pi i m z}.$$

All in all, this yields

$$\lambda(n) a(1) = a'(1) = a(n),$$

as asserted. ■

Remark. Let $0 \neq f \in \mathcal{S}_k(\Gamma)$ be a Hecke eigenform. By the previous Proposition, we then have

$$a(1) \neq 0,$$

since otherwise $f = 0$. Furthermore, f is uniquely determined by the eigenvalues $\lambda(1), \lambda(2), \ldots$.
Similarly, for a non-constant Hecke eigenform $0 \neq f \in \mathcal{M}_k(\Gamma)$, we have

$$a(1) \neq 0,$$

since otherwise f would be a constant.

Definition 5.16. A Hecke eigenform f is called *normalized Hecke eigenform*, if $a(1) = 1$. We then have $a(n) = \lambda(n)$ for all $n \in \mathbb{N}_{\geq 1}$, thus the Hecke eigenvalues $\lambda(n)$ are precisely the coefficients an in the q-expansion of f.

Proposition 5.17. Let $f \in \mathcal{M}_k(\Gamma)$ be a non-constant modular form, with Fourier expansion $f(z) = \sum_{m=0}^{\infty} a(m)q^m$. Then, f is a normalized Hecke eigenform if and only if the Fourier coefficients $a(m)$ of f satisfy

$$a(m)a(n) = \sum_{d \,|\, (m,n)} d^{k-1} a\left(\frac{mn}{d^2}\right), \tag{5.3}$$

for all $m \in \mathbb{N}$ and $n \in \mathbb{N}_{\geq 1}$.

Proof. Let $f \in \mathcal{M}_k(\Gamma)$ be a non-constant modular form, with Fourier expansion

$$f(z) = \sum_{m=0}^{\infty} a(m)q^m. \tag{5.4}$$

Recall that, for $n \in \mathbb{N}_{\geq 1}$, by Remark 5.1 we have

$$f|T(n)(z) = \sum_{m=0}^{\infty} a'(m)q^m \tag{5.5}$$

with

$$a'(m) := \sum_{d \,|\, (m,n)} d^{k-1} a\left(\frac{mn}{d^2}\right).$$

In particular, we have

$$a'(0) = \sigma_{k-1}(n)a(0) \qquad \text{and} \qquad a'(1) = a(n).$$

Now, assume that f is a normalized Hecke eigenform, with $f|T(n) = \lambda(n)f$ for all $n \in \mathbb{N}_{\geq 1}$. We have $a(n) = \lambda(n)$ for all $n \in \mathbb{N}_{\geq 1}$. Thus, comparing (5.4) with (5.5), we get

$$a(0)a(n) = a(0)\lambda(n) = a'(0) = \sigma_{k-1}(n)a(0) = \sum_{d \,|\, n} d^{k-1}a(0),$$

for all $n \in \mathbb{N}_{\geq 1}$, which proves (5.3) for $m = 0$. Next, by Corollary 5.8, the eigenvalues satisfy

$$\lambda(m)\lambda(n) = \sum_{d \,|\, (m,n)} d^{k-1} \lambda\left(\frac{mn}{d^2}\right),$$

for $m, n \in \mathbb{N}_{\geq 1}$. Since $a(n) = \lambda(n)$ for all $n \in \mathbb{N}_{\geq 1}$, this yields the claimed relation (5.3) for $m, n \in \mathbb{N}_{\geq 1}$.
Now, assume that the Fourier coefficients of f satisfy (5.3), i.e.

$$a(m)a(n) = \sum_{d \mid (m,n)} d^{k-1} a\left(\frac{mn}{d^2}\right),$$

for all $m \in \mathbb{N}$ and $n \in \mathbb{N}_{\geq 1}$. For $n = 1$, this yields

$$a(m)a(1) = a(m),$$

for all $m \in \mathbb{N}_{\geq 1}$. Since f is non-constant, not all of the $a(m)$'s vanish, hence we get $a(1) = 1$. Furthermore, for all $m \in \mathbb{N}$ and $n \in \mathbb{N}_{\geq 1}$, we get

$$a'(m) = \sum_{d \mid (m,n)} d^{k-1} a\left(\frac{mn}{d^2}\right) = a(m)a(n),$$

hence

$$f|T(n) = a(n)f,$$

for all $n \in \mathbb{N}_{\geq 1}$. This completes the proof. ■

▪ **Example 5.18.** The following examples can be proven as exercise:
(a) $\Delta(z) \in \mathcal{S}_{12}(\Gamma)$ is a normalized Hecke eigenform.
(b) $E_k(z) \in \mathcal{M}_k(\Gamma)$ is a Hecke eigenform.

▪

We now finally prove the self-adjointness of the Hecke operators with respect to the Petersson scalar product.

Proposition 5.19. Let $n \in \mathbb{N}_{\geq 1}$. For all $f, g \in \mathcal{S}_k(\Gamma)$, we have

$$\langle f|T(n), g \rangle = \langle f, g|T(n) \rangle,$$

i.e. the Hecke operator $T(n)$ is selfadjoint with respect to the Petersson scalar product.

Proof. Without loss of generality we may assume $k \geq 12$. Let $f \in \mathcal{S}_k(\Gamma)$ and let $a(m)$ ($m \in \mathbb{N}_{\geq 1}$ denote the Fourier coefficients of f. Then, also $f|T(n) \in \mathcal{S}_k(\Gamma)$; let $a'(m)$ ($m \in \mathbb{N}_{\geq 1}$ denote the Fourier coefficients of $f|T(n)$.
By Proposition 5.13, it suffices to prove the assertion for g being equal to the Poincaré series $P_{m,k}$ with $m \in \mathbb{N}_{\geq 1}$. We compute

$$\begin{aligned}
\langle f|T(n), P_{m,k} \rangle &= \frac{(k-2)!}{(4\pi m)^{k-1}} a'(m) \\
&= \frac{(k-2)!}{(4\pi m)^{k-1}} \sum_{d \mid (m,n)} d^{k-1} a\left(\frac{mn}{d^2}\right) \\
&= \frac{(k-2)!}{(4\pi m)^{k-1}} \sum_{d \mid (m,n)} d^{k-1} \frac{(4\pi \frac{mn}{d^2})^{k-1}}{(k-2)!} \langle f, P_{\frac{mn}{d^2},k} \rangle \\
&= \langle f, \sum_{d \mid (m,n)} \frac{n^{k-1}}{d^{k-1}} P_{\frac{mn}{d^2},k} \rangle.
\end{aligned}$$

Here, for the first equality we used Proposition 5.13, for the second equality we used (5.2), and for the third equality we used again Proposition 5.13. The proof is complete by showing that

$$P_{m,k}|T(n) = \sum_{d\,|\,(m,n)} \frac{n^{k-1}}{d^{k-1}} P_{\frac{mn}{d^2},k},$$

for $m, n \in \mathbb{N}_{\geq 1}$. This can be shown similarly as for the Eisenstein series E_k, and is left as exercise for the reader. ■

Proposition 5.20. The vector space $\mathcal{S}_k(\Gamma)$ has a basis consisting of Hecke eigenforms.

Proof. The existence of a basis of $\mathcal{S}_k(\Gamma)$ of Hecke eigenforms follows by known facts from linear algebra (spectral theory), since $\mathcal{H}$ is a commutative algebra, consisting of self-adjoint operators. ■

More precicely: we may decompose $\mathcal{S}_k(\Gamma)$ as a direct sum of eigenspaces V_j for the Hecke operators $T(n)$. Let $f = \sum a(n)q^n \in V_j$, $f \neq 0$. For the first Fourier coefficient $a'(1)$ of $f \mid T(n)$, we have

$$a'(1) = a(n).$$

Also $f \mid T(n) = \lambda_n f$ for some eigenvalue λ_n of $T(n)$ which is determined by V_j, so

$$a(n) = \lambda_n a(1).$$

This implies $a(1) \neq 0$, since otherwise $f = 0$, and if we normalize f so that $a_1 = 1$. We then have

$$a(n) = \lambda_n a(1).$$

and f is completely determined by the sequence of Hecke eigenvalues λ_n for V_j. It follows that every element of V_j is a multiple of f, so $\dim(V_j) = 1$ and the eigenforms in $\mathcal{S}_k(\Gamma)$ form a basis.

Theorem 5.21 The vector space $\mathcal{S}_k(\Gamma)$ can be written as a direct sum of one-dimensional eigenspaces for the Hecke operators $T(n)$ and has a unique basis of eigenforms f, where each $a(n)$ is the eigenvalue of $T(n)$ on the 1-dimensional subspace generated by f.

5.2 Hecke Operators for $\mathcal{M}_k(\Gamma_0(N))$

In the previous section, we have studied Hecke operators for $\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(1)$. In this section, we mention some results for $\Gamma_0(N)$ with $N \geq 1$.

From the previous section, we recall (see in particular Corollary 5.5) that

Proposition 5.22. (i) Let $f \in \mathcal{S}_k(\Gamma_0(1))$ and p be a prime. Then, the m-th Fourier coefficient $a'(m)$ of $f \mid T(p)$ $(m \in \mathbb{N})$ satisfies the identity

$$a'(m) = a(mp) + p^{k-1} a\left(\frac{m}{p}\right),$$

where we have set $a(\frac{m}{p}) := 0$, if $\frac{m}{p} \notin \mathbb{Z}$.
(ii) Let $f \in \mathcal{S}_k(\Gamma_0(1))$ and let $m, n \in \mathbb{N}$ be relatively prime. Then, the m-th Fourier

coefficient $a'(m)$ of $f \mid T(n)$ satisfies the identity

$$a'(m) = a(mn).$$

In particular

$$a'(1) = a(n).$$

Remark. All these results also hold $f \in \mathcal{S}_k(\Gamma_0(N))$, if we restrict to Hecke operators $T(n)$ with $(n, N) = 1$, which is all that we require, and the key result

$$a'(1) = a(n).$$

holds in general.

Remark. For $p \mid N$, the definition of $T(p)$ (and $T(n)$ for $p \mid n$) needs to change and the formulas in Proposition 5.22 must be modified. The definition of the Hecke operators is more complicated (in particular, it depends on the level N), but some of the formulas are actually simpler (for example, for $p \mid N$ we have $T(p^r) = T(p)^r$).

Also, we have seen

Theorem 5.23 The vector space $\mathcal{S}_k(\Gamma)$ can be written as a direct sum of one-dimensional eigenspaces for the Hecke operators $T(n)$ and has a unique basis of eigenforms f, where each $a(n)$ is the eigenvalue of $T(n)$ on the 1-dimensional subspace generated by f.

An analoge of Theorem 5.23 doesn't hold for $\mathcal{S}_k(\Gamma_0(N))$. We need to restrict our attention to the Hecke operators $T(n)$ with $(n, N) = 1$ (when n and N have a common factor $T(n)$ is not necessarily a Hermitian operator with respect to the Petersson inner product).
We can then proceed as above to decompose $\mathcal{S}_k(\Gamma_0(N))$ into subspaces whose elements are simultaneous eigenvectors for all the $T(n)$ with $(n, N) = 1$, but these subspaces need not be one-dimensional.
In order to ensure this, we restrict our attention to a particular subspace of $\mathcal{S}_k(\Gamma_0(N))$. We recall that a cusp form $f \in \mathcal{S}_k(\Gamma_0(N))$ is an oldform if it also lies in $\mathcal{S}_k(\Gamma_0(M))$ for some $M|N$, which is a subspace of $\mathcal{S}_k(\Gamma_0(N))$. The oldforms in $\mathcal{S}_k(\Gamma_0(N))$ generate a subspace

$$\mathcal{S}_k^{\text{old}}(\Gamma_0(N)).$$

Definition 5.24. Let $f, g \in \mathcal{M}_k(\Gamma_0(N))$, where at least one of them is a cusp form. Then, the *Petersson scalar product of f and g* is defined by

$$\langle f, g \rangle := \int\limits_{\Gamma_0(N)\backslash\mathbb{H}} f(z)\overline{g(z)}\text{Im}(z)^k \mu_{\text{hyp}}(z),$$

where $z = x + iy$ and $\mu_{\text{hyp}}(z) = dxdy/y^2$.

Definition 5.25. We define $\mathcal{S}_k^{\text{new}}(\Gamma_0(N))$ to be the orthogonal complement of $\mathcal{S}_k^{\text{old}}(\Gamma_0(N))$ with respect to the Petersson inner product, so that

$$\mathcal{S}_k(\Gamma_0(N)) = \mathcal{S}_k^{\text{old}}(\Gamma_0(N)) \oplus \mathcal{S}_k^{\text{new}}(\Gamma_0(N)).$$

The eigenforms in $\mathcal{S}_k^{\text{new}}(\Gamma_0(N))$ are called *newforms*.

Remark. One can show that the Hecke operators $T(n)$ with $(n,N) = 1$ preserve both $\mathcal{S}_k^{\text{old}}(\Gamma_0(N))$ and $\mathcal{S}_k^{\text{new}}(\Gamma_0(N))$. If we then decompose $\mathcal{S}_k^{\text{new}}(\Gamma_0(N))$ into eigenspaces with respect to these operators, the resulting eigenspaces are all one-dimensional, moreover, each is actually generated by an eigenform (a simultaneous eigenvector for all the $T(n)$, not just those with $(n,N) = 1$ that we used to obtain the decomposition); this is a famous result of Atkin and Lehner. Thus Theorem 5.23 remains true if we simply replace $\mathcal{S}_k(\Gamma_0(1))$ by $\mathcal{S}_k^{\text{new}}(\Gamma_0(N))$.

At the end of this section, let us collect some facts for $k = 2$ und $\mathcal{S}_2(\Gamma_0(N))$. The Petersson scalar product of $f, g \in \mathcal{S}_2(\Gamma_0(N))$ is given by

$$\langle f, g\rangle := \int\limits_{\Gamma_0(N)\backslash\mathbb{H}} f(z)\overline{g(z)}dxdy,$$

where $z = x + iy$.

For $n \in \mathbb{Z}$, the Hecke operators $T(n)$ are defined as follows:

Definition 5.26. Let p be a prime. If $p \nmid N$, we set

$$f|T(p)(z) := \frac{1}{p}\sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) + pf(pz).$$

If $p \mid N$, we set

$$f|T(p)(z) := \frac{1}{p}\sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right).$$

These operators act linearly on $\mathcal{S}_2(\Gamma_0(N))$ and we have

Proposition 5.27. If $p \nmid N$, we have

$$f|T(p)(z) = \sum_{p|n} a(n)q^{n/p} + p\sum_{n\geq 1} a(n)q^{pn}.$$

If $p \mid N$, we have

$$f|T(p)(z) = \sum_{p|n} a(n)q^{n/p}.$$

Definition 5.28. Let p be a prime. For $n > 0$, we set

$$T(p^{n+1})(z) := T(p)(z)T(p^n)(z) - pT(p^{n-1})(z)$$

If $n = \prod_j p_j^{e_j}$ is a prime factorization, we set

$$f|T(n)(z) := \prod_j T(p_j^{e_j})(z).$$

Definition 5.29. We define the Hecke Algebra $\mathcal{H}$ of $\mathcal{S}_2(\Gamma_0(N))$ as $\mathbb{Z}[T(1), T(2), T(3), \ldots]$.

Remark. Let $M \in \mathbb{N}_{>0}$ with $M \mid N$ and let $f \in \mathcal{S}_2(\Gamma_0(M))$. Let $d \in \mathbb{N}_{>0}$ with $d \mid \frac{N}{M}$.

Then, we have seen that $f(dz) \in \mathcal{S}_2(\Gamma_0(N))$. The map

$$\beta_d : \mathcal{S}_2(\Gamma_0(M)) \to \mathcal{S}_2(\Gamma_0(N)), f(z) \mapsto f(dz)$$

called the *d-degeneracy map from level M*. On Fourier coefficients, we have

$$\beta_d : \mathcal{S}_2(\Gamma_0(M)) \to\in \mathcal{S}_2(\Gamma_0(N)), \sum_{n=1}^{\infty} a(n)q^n \mapsto \sum_{n=1}^{\infty} a(n)q^{dn}.$$

Remark. The old subspace $\mathcal{S}_2^{\text{old}}(\Gamma_0(N))$ is then the subspace of cusp forms that are images of degeneracy maps from all levels $M \mid N$.

Theorem 5.30 — (Atkin–Lehner). We have

$$\mathcal{S}_2(\Gamma_0(N)) = \mathcal{S}_2^{\text{old}}(\Gamma_0(N)) \oplus_\lambda \mathbb{C} f_\lambda,$$

where the sum is taken over all algebra homomorphisms $\lambda : \mathcal{H} \to \mathbb{C}$, corresponding to eigenforms in $\mathcal{S}_2^{\text{new}}(\Gamma_0(N))$, and

$$f_\lambda = \sum_{n=1}^{\infty} \lambda(T(n))q^n.$$

Remark. The simultaneous eigenvector f_λ is sometimes simply called *newform of level N*.

6. Appendix: Eisenstein series

Definition 6.1. Let $k \geq 4$ be an even integer. Then the series

$$G_k(z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^k} =: \sideset{}{'}\sum_{(m,n)\in\mathbb{Z}^2} \frac{1}{(mz+n)^k}$$

is called *Eisenstein series of weight k*.

Lemma 6.2. The series

$$\sideset{}{'}\sum_{(m,n)\in\mathbb{Z}^2} \frac{1}{(m^2+n^2)^s}$$

converges for real $s > 1$.

Proof. Since all terms are positive, it suffices to prove the convergence of

$$\sum_{m=1}^{\infty}\sum_{n=1}^{m-1} \frac{1}{(m^2+n^2)^s},$$

since the $m < n$ terms give the same contribution to the sum as the $m > n$ terms and $m = n$ leads to

$$\sum_{m=1}^{\infty} \frac{1}{(2m^2)^s} = \frac{1}{2^s}\zeta(2s),$$

where $\zeta(\cdot)$ denotes the Riemann zeta function.
So, let $m \geq 1$. Then

$$\sum_{n=1}^{m-1} \frac{1}{(m^2+n^2)^s} \leq \frac{(m-1)}{m^{2s}} < \frac{1}{m^{2s-1}}.$$

Therefore

$$\sum_{m=1}^{\infty}\sum_{n=1}^{m-1} \frac{1}{(m^2+n^2)^s} < \sum_{m=1}^{\infty} \frac{1}{m^{2s-1}} = \zeta(2s-1).$$

Hence, the series under consideration converges absolutely for $2s-1>1$ ($\iff s>1$). This proves the claim. ■

Proposition 6.3. Let $k \geq 4$ be an even integer. Then, the series $G_k(z)$ converges absolutely and locally uniformly on $\mathbb{H}$, hence it defines a holomorphic function $G_k : \mathbb{H} \longrightarrow \mathbb{C}$. For any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we have

$$G_k(\gamma z) = (cz+d)^k G_k(z)$$

and therefore $G_k(z)$ is a weak modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$.

Proof. It suffices to show that the series defining $G_k(z)$ converges absolutely and locally uniformly on

$$R_{\delta,C} := \{z = x+iy \in \mathbb{H} \mid |x| \leq C,\ y > \delta\}$$

for all $\delta > 0$, $C > 0$ (since, for $C \to \infty$ and $\delta \to 0$, the interior of this set fills all of $\mathbb{H}$). We will show that for all $\delta > 0$, $C > 0$, there exists $\varepsilon > 0$ such that for all $m, n \in \mathbb{R}$ and all $z \in R_{\delta,C}$ we have

$$|mz+n|^2 \geq \varepsilon(m^2+n^2).$$

This follows from the following inequality: for $\delta > 0$, $C > 0$ there exists $\varepsilon > 0$ such that for all $m, n \in \mathbb{R}$ with $m^2+n^2 = 1$ and all $z \in R_{\delta,C}$:

$$|mz+n|^2 \geq \varepsilon$$

(just divide m and n by $\sqrt{m^2+n^2}$). For $m = n = 0$, the inequality is trivial.
For $z = x+iy \in R_{\delta,C}$ we get

$$|mz+n|^2 = (mx+n)^2 + (my)^2 > (mx+n)^2 + m^2\delta^2 > 0.$$

Since the set $\{(m,n,x) \in \mathbb{R}^3 \mid m^2+n^2 = 1,\ |x| \leq C\}$ is compact, the continuous function $(mx+n)^2 + m^2\delta^2$ attains its minimum. We choose ε to be this minimum.
Therefore, we have the bound

$$\sum_{(m,n)\in\mathbb{Z}^2}{}' \left|\frac{1}{(mz+n)^k}\right| \leq \frac{1}{\varepsilon^{k/2}} \sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{(m^2+n^2)^{k/2}} < \infty$$

for all $z \in R_{\delta,C}$, using Lemma 6.2 and recalling that $k/2 > 1$. This proves the convergence claim.

Now, for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we compute (by reordering in the 4th step)

$$\begin{aligned}
G_k(\gamma z)(cz+d)^{-k} &= \sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{(m\frac{az+b}{cz+d}+n)^k}(cz+d)^{-k} \\
&= \sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{(m(az+b)+n(cz+d))^k} \\
&= \sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{((ma+nc)z+(mb+nd))^k} \\
&= \sum_{(m',n')\in\mathbb{Z}^2}{}' \frac{1}{(m'z+n')^k} \\
&= G_k(z).
\end{aligned}$$

This finishes the proof. ■

Remark. The series $G_k(z)$ is a modular form for $\mathrm{SL}_2(\mathbb{Z})$, since in this case being "holomorphic at the cusps of $\mathrm{SL}_2(\mathbb{Z})$" means that the q-series of $G_k(z)$ is of the form

$$G_k(z) = \sum_{n=0}^{\infty} a_n q^n.$$

We will now compute the q-series of $G_k(z)$. To do this, we will use the following facts.

Remark. Let $k \geq 4$ be an even integer. Due to the absolute convergence, we can write

$$G_k(z) = 2\zeta(k) + 2\sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k},$$

where $\zeta(\cdot)$ denotes the Riemann zeta function, and we have the identities (for a proof, see Proposition 6.8)

$$\zeta(2) = \frac{\pi^2}{6}, \qquad \zeta(4) = \frac{\pi^2}{90}, \qquad \zeta(6) = \frac{\pi^6}{945}.$$

Lemma 6.4. Let $k \geq 2$ be an integer. Define, for $n \in \mathbb{N}$, the powers-of-divisor-sum

$$\sigma_{k-1}(n) := \sum_{\substack{d \mid n \\ 1 \leq d \leq n}} d^{k-1}. \tag{6.1}$$

Then, the series

$$\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \qquad (q = e^{2\pi i z})$$

defines a holomorphic function on $\mathbb{H}$ and equals

$$\sum_{n=1}^{\infty} \sum_{m=1}^{\infty} n^{k-1} q^{mn}.$$

Proof. We have $\sigma_{k-1}(n) \leq n n^{k-1} \leq n^k$. To prove the first claim, it suffices to prove that $\sum_{n=1}^{\infty} n^k q^n$ defines a holomorphic function on $\mathbb{H}$. This is easily verified by using the ratio test. The second claim follows by reordering and collecting all the terms with the same mn. ∎

Lemma 6.5. Let $k \geq 2$ be an integer. Then, the following identity of absolutely and uniformly converging series holds:

$$(-1)^k \sum_{n=-\infty}^{\infty} \frac{1}{(z+n)^k} = \frac{1}{(k-1)!} (2\pi i)^k \sum_{n=1}^{\infty} n^{k-1} q^n.$$

Proof. First let $k = 2$. We have to show that

$$\sum_{n=-\infty}^{\infty} \frac{1}{(z+n)^2} = (2\pi i)^2 \sum_{n=1}^{\infty} n q^n. \tag{6.2}$$

We first recall that, for $z \in \mathbb{C} \setminus \mathbb{Z}$, we have

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z+n} + \frac{1}{z-n} \right) \tag{6.3}$$

and the series converges absolutely and locally uniformly. Using the series expansion (6.3), we then compute

$$\begin{aligned}\frac{d}{dz}(\pi\cot(\pi z)) &= -\frac{1}{z^2} - \sum_{n=1}^{\infty}\left(\frac{1}{(z+n)^2} + \frac{1}{(z-n)^2}\right)\\ &= -\sum_{n=-\infty}^{\infty}\frac{1}{(z+n)^2}.\end{aligned}$$

Further, we have

$$\begin{aligned}\pi\cot(\pi z) &= \pi\frac{\cos(\pi z)}{\sin(\pi z)} = \pi i\frac{e^{\pi iz}+e^{-\pi iz}}{e^{\pi iz}-e^{-\pi iz}}\\ &= \pi i\frac{q+1}{q-1} = \pi i - 2\pi i\frac{1}{1-q}\\ &= \pi i - 2\pi i\sum_{n=0}^{\infty}q^n.\end{aligned}$$

Hence

$$\frac{d}{dz}\pi\cot(\pi z) = -2\pi i\sum_{n=1}^{\infty}nq^{n-1}2\pi i\, q = -(2\pi i)^2\sum_{n=1}^{\infty}nq^n.$$

This proves (6.2).

The case $k \geq 4$ is obtained by differentiating the identity in (6.2) $k-2$ times. ■

Collecting the above facts, we can prove the following proposition, yielding in particular the Fourier expansion of $G_k(z)$ for $k \geq 4$.

Proposition 6.6. Let $k \geq 2$ be an even integer. We have the following identity of holomorphic functions on $\mathbb{H}$:

$$2\zeta(k) + 2\sum_{m=1}^{\infty}\left(\sum_{n=-\infty}^{\infty}\frac{1}{(mz+n)^k}\right) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n.$$

If $k \geq 4$, this function equals $G_k(z)$. If $k = 2$, this function will be denoted by $P(z)$ and is called Ramanujan P-function.
In particular, we have

$$\begin{aligned}P(z) &= -8\pi^2\left(-\frac{1}{24} + \sum_{n=1}^{\infty}\sigma_1(n)q^n\right)\\ G_4(z) &= \frac{16}{3}\pi^4\left(\frac{1}{240} + \sum_{n=1}^{\infty}\sigma_3(n)q^n\right)\\ G_6(z) &= -\frac{16}{15}\pi^6\left(-\frac{1}{504} + \sum_{n=1}^{\infty}\sigma_5(n)q^n\right),\end{aligned}$$

recalling that $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$ and $\zeta(6) = \frac{\pi^6}{945}$ (cf. Proposition 6.8).

Proof. We consider the left hand side and apply the result of Lemma 6.5 with $z = mz$ (and observe that for even k the factor $(-1)^k$ can be omitted), namely the following identity of absolutely and uniformly converging series

$$\begin{aligned}\sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k} &= \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} e^{2\pi i n(mz)} \\ &= \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^{mn}.\end{aligned}$$

We get

$$\begin{aligned}2\zeta(k) + 2\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k} &= 2\zeta(k) + 2\frac{(2\pi i)^k(-1)^k}{(k-1)!} \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n^{k-1} q^{mn} \\ &= 2\zeta(k) + 2\frac{(2\pi i)^k(-1)^k}{(k-1)!} \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} n^{k-1} q^{mn},\end{aligned}$$

where for the last equality we used that the series is absolutely converging. Applying Lemma 6.4, namely the identity

$$\sum_{n=1}^{\infty}\sum_{m=1}^{\infty} n^{k-1} q^{mn} = \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

yields the claim. ■

Remark. If $k = 2$, we are not allowed to reorder the series on the left hand side in Proposition 6.6.

Finally, we recall the definition of the Bernoulli numbers.

Definition 6.7. We consider the function

$$\frac{z}{e^z - 1} = \frac{z}{\sum_{n=1}^{\infty} \frac{z^n}{n!}} = \frac{1}{\sum_{n=0}^{\infty} \frac{z^n}{(n+1)!}}$$

which is thus holomorphic at 0. We write its Taylor series of $z/(e^z - 1)$ at $z = 0$ in the following form

$$\frac{z}{e^z - 1} = \sum_{k=0}^{\infty} \frac{B_k}{n!} z^n.$$

The coefficients B_k $(k \in \mathbb{N})$ arising in this expansion are called *Bernoulli numbers*.

Remark. One easily proves the relation

$$\binom{n+1}{1} B_n + \binom{n+1}{2} B_{n-1} + \ldots + \binom{n+1}{n} B_1 + \binom{n+1}{n+1} B_0 = 0.$$

Hence

$$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_3 = 0,\ B_4 = -\frac{1}{30},\ B_6 = \frac{1}{42}$$

and $B_k = 0$ for all odd $k \geq 3$.

Proposition 6.8. — Euler. For $k \in \mathbb{N}$, $k > 0$, we have

$$\zeta(2k) = \frac{(-1)^{k+1}(2\pi)^{2k}}{2(2k)!} B_{2k}. \tag{6.4}$$

In particular, we have

$$\zeta(2) = \frac{\pi^2}{6},\ \zeta(4) = \frac{\pi^4}{90},\ \zeta(6) = \frac{\pi^6}{945}.$$

Proof. The idea of proof consists in comparing two different series representations of the function $\pi z \cot(\pi z)$. We start with the identity given in (6.3) (multiplied with z), namely

$$\pi z \cot(\pi z) = 1 + \sum_{n=1}^{\infty} \left(\frac{z}{z+n} + \frac{z}{z-n} \right),$$

for $z \in \mathbb{C} \setminus \mathbb{Z}$. The above series is absolutely and locally uniformly convergent on $\mathbb{C} \setminus \mathbb{Z}$. Hence, we get

$$\pi z \cot(\pi z) = 1 + 2z^2 \sum_{n=1}^{\infty} \frac{1}{z^2 - n^2}.$$

Using the geometric series, for z in a neighbourhood of 0, we can write

$$\frac{1}{z^2-n^2} = -\frac{1}{n^2} \frac{1}{1-(z^2/n^2)} = -\frac{1}{n^2} \sum_{k=0}^{\infty} \left(\frac{z^2}{n^2} \right)^k$$

and we obtain

$$\pi z \cot(\pi z) = 1 + 2z^2 \sum_{n=1}^{\infty} \left(-\frac{1}{n^2} \sum_{k=0}^{\infty} \left(\frac{z^2}{n^2} \right)^k \right).$$

This series converges locally absolutely in a neighbourhood of 0, since for positive $z \notin \mathbb{Z}$ all terms are positive. Therefore we can interchange the sums and we get the first expression

$$\begin{aligned}
\pi z \cot(\pi z) &= 1 - 2 \sum_{k=0}^{\infty} \left(\sum_{n=1}^{\infty} \frac{1}{n^{2k+2}} \right) z^{2k+2} \\
&= 1 - 2 \sum_{k=1}^{\infty} \left(\sum_{n=1}^{\infty} \frac{1}{n^{2k}} \right) z^{2k} \\
&= 1 - 2 \sum_{k=1}^{\infty} \zeta(2k) z^{2k}.
\end{aligned}$$

A second expression for $\pi z \cot(\pi z)$ is obtained by writing

$$\cot(\pi z) = i \frac{e^{\pi i z} + e^{-\pi i z}}{e^{\pi i z} - e^{-\pi i z}} = i \frac{e^{2\pi i z} + 1}{e^{2\pi i z} - 1} = i + \frac{2i}{e^{2\pi i z} - 1},$$

whence

$$\pi z \cot(\pi z) = \pi i z + \frac{2\pi i z}{e^{2\pi i z} - 1}.$$

The last term can now be written in terms of the Bernoulli numbers, namely, we have

$$\begin{aligned}
\pi z \cot(\pi z) &= \pi i z + \sum_{k=0}^{\infty} \frac{B_k}{k!} (2\pi i z)^k \\
&= 1 + \sum_{k=1}^{\infty} \frac{B_{2k}}{(2k)!} (2\pi i z)^{2k} \\
&= 1 + \sum_{k=1}^{\infty} \frac{B_{2k}}{(2k)!} 2^{2k} \pi^{2k} (-1)^k z^{2k},
\end{aligned}$$

where we used that $B_0 = 1$, $B_1 = -\frac{1}{2}$ and $B_k = 0$ for odd $k \geq 3$. Comparing the coefficients now yields the assertion. ■